TRUTHFUL RESOURCE MANAGEMENT IN WIRELESS AD HOC NETWORKS

A Dissertation

by

JIANFENG CAI

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

August 2005

Major Subject: Computer Science

TRUTHFUL RESOURCE MANAGEMENT IN WIRELESS AD HOC NETWORKS

A Dissertation

by

JIANFENG CAI

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Approved by:

Co-Chairs of Committee,	Udo Pooch
	Riccardo Bettati
Committee Members,	Jianer Chen
	Michael Longnecker
	Rabi N. Mahapatra
Head of Department,	Valerie E. Taylor

August 2005

Major Subject: Computer Science

ABSTRACT

Truthful Resource Management in Wireless Ad Hoc Networks. (August 2005)

Jianfeng Cai, B.E., National University of Defense Technology

Co–Chairs of Advisory Committee: Dr. Udo Pooch
Dr. Riccardo Bettati

In wireless mobile ad hoc networks (MANETs), cooperation cannot be an implicit assumption anymore. Each profit-oriented network node has the intention to be selfish due to limited resource possession. In this dissertation, we investigate the truthful resource management that induces network nodes to reveal true information and stimulate cooperation.

We propose the Transmission Power Recursive Auction Mechanism routing protocol (TEAM) and the Truthful Topology Control mechanism (TRUECON) to cope with the selfish intention and achieve resource efficiency in a non-cooperative environment. We prove both are strategy-proof and have some theoretic bounds on the performance. Compared with the existing routing protocols and topology control algorithms, TEAM and TRUECON are more efficient when dealing with the selfishness in MANETs.

We conduct a study on anonymity enhancement in MANETs by reducing transmission power of network nodes. A routing protocol - Whisper is presented. Simulation results show that it has desirable properties in terms of anonymity and power efficiency.

To my parents, Deming Cai and Zongming Yang, and my wife, Yue Chen

TABLE OF CONTENTS

CHAPTER Page

LIST OF TABLES

LIST OF FIGURES

FIGURE Page

FIGURE Page

CHAPTER I

INTRODUCTION

A. Motivation

Wireless mobile ad hoc networking (MANET) technology enables users to form a communication network on the fly. In a MANET, any portable device with a radio component can communicate with others without the aid of pre-deployed infrastructures. "Communicating anytime and anywhere" is always a fascinating idea for people.

Due to the limited resource possession, especially the energy, of mobile nodes, how to manage the resource usage efficiently is very important. Many efforts [1, 2, 3, 4, 5, 6, 7] have been made on energy-efficient routing. Adjusting the transmission power to induce a power-efficient network topology is also studied extensively in [8, 9, 10, 11, 12, 13, 14, 15].

Underneath these researches lies a common assumption that every node in a MANET always does exactly what it is supposed to do. Ironically, as mobile communication technologies bring the freedom of staying in touch, they also bring the freedom of breaking rules. Network nodes in MANETs are usually managed by different profit-oriented entities, such as people belonging to different groups or companies. As a result they follow their own interests instead of any pre-defined procedures.

Selfish behaviors are inevitable in MANETs due to the lack of a central authority and the limited amount of critical resources. Any protocol cannot assume that all network nodes strictly follow its guidelines. Researchers have tackled the selfishness from two approaches. One is to treat selfish nodes as a security threat and try to identify and punish them. Efforts in [16, 17, 18, 19] belong to this category. However,

---

The journal model is *IEEE Transactions on Automatic Control*.

selfish nodes are different from malicious nodes though they may degrade the network performance like malicious nodes. Selfish nodes are *rational* in that they are only interested in maximizing their own benefits rather than attacking others.

Another approach is to stimulate cooperation by creating incentives. Research works [20, 21, 22, 23, 24, 25] in this category study the economic implication of the resource management problem.

From the game-theoretic perspective, we can model a network node v as an independent agent in a game. The preference of v is represented as a utility function u_v. It consists of two parts: one is the cost of a network activity the node participates; another is the payoff for v by the participation. Without any payment transfer, v has a non-positive utility when it forwards data packets for other nodes. It is because it drains its own energy to serve others. Consequently, the best strategy for v is to refuse any forwarding request and have the maximum utility at 0. Therefore, any protocol ignoring a node's selfish intention and treating a MANET as a collaborative system will fall short to achieve its goals.

Apparently, if we can design a mechanism for network nodes in a MANET and convince them that following rules of the mechanism can best serve their interests, collaborations may prevail in such a non-cooperative environment. Such a mechanism is called a *strategy-proof* mechanism or a *truthful* mechanism, because any node cannot trick the mechanism to get an outcome in favor of its own utility.

Designing truthful mechanisms to stimulate collaborations in a non-cooperative MANET is the motivation of this research. In the last part of this dissertation, we expand the meaning of being truthful to the protection of user privacy. We conduct a study on enhancing anonymous communication in MANETs.

B. Main Contributions

In this dissertation we identify the importance of the incentive of network nodes. Based on this observation, we design two truthful mechanisms for routing and conducting topology control in MANETs respectively. We also extend the research to power-efficient user privacy protection. Our main contributions can be classified into three categories.

- We design the Transmission Power Recursive Auction Mechanism (TEAM) routing protocol to discover power-efficient paths in a MANET of selfish nodes. We prove TEAM achieves truthfulness. In term of efficiency, TEAM is an approximate algorithm. With some conditions, we prove that the power efficiency along a TEAM path can be bounded within a certain range comparing to the optimal solution. We show TEAM has a lower message complexity than another truthful routing protocol – Ad hoc – VCG [22].

- We propose a truthful topology control mechanism - Truthful Topology Control (TRUECON), which is a pioneering work in MANETs. Inducing network nodes to reveal their true cost and generate an appropriate topology is a promising direction for truthful resource management in non-cooperative MANETs. TRUECON preserves the network connectivity while keeping the node degree as a constant and reducing the average transmission range significantly. We demonstrate TRUECON achieves all these objectives along with the truthfulness.

  We simulate TRUECON with DSR [26] ad hoc routing protocol and evaluate the system performance by applying various metrics. The result is satisfactory.

- We study enhancing anonymous communication in MANETs by reducing the

transmission power of network nodes and propose a routing protocol - Whisper. In certain scenarios, Whisper gives the communication initiator a better chance to hide among its peer nodes.

C. Dissertation Structure

The remainder of this dissertation is organized as follows. Next chapter introduces the technical background, including game theory, mechanism design, and radio propagation characteristics. The network model we assume throughout our work is also presented in this chapter.

Chapter III discusses the truthful routing and proposes TEAM protocol in detail. We prove the truthfulness of the protocol and analyze its efficiency comparing to an optimal solution.

In Chapter IV, we discuss the design, implementation and evaluation of a truthful topology control mechanism – TRUECON.

We summarize our contributions and draw conclusions in Chapter V. We also identify challenges and point out the direction for future work.

In Appendix A, we study anonymous communication in MANETs and propose a routing protocol – Whisper to enhance anonymity of communication initiators in some network circumstances. Appendix B presents the simulation data of experiments we conduct in this dissertation.

CHAPTER II

BACKGROUND

A. Game Theory and Mechanism Design

Game theory [27, 28, 29] is a method to study the conflicts and the behaviors of players based on the strategy interaction. The objects, which act independently in a game, are also called agents. In the rest of this dissertation, agent and player are exchangeable. Each player has its preference, called type, over the outcome of a game. The type is private information of every player. A type of player i is denoted as $\theta_i \in \Theta_i$ from a set of types Θ_i. Given an outcome o of a game from a set of outcome O, the utility of agent i is $u(o, \theta_i)$.

Definition A.1 *A strategy s_i is a plan of actions agent i takes under a specific state in a game.*

An agent has a set of strategies S_i. The outcome of a game, $o(s_1, \ldots, s_n)$, depends on the input of strategies of all the participating agents. Thus if agent i prefers a strategy s_i to s'_i, $u(o(s_1, \ldots, s_i, \ldots, s_n), \theta_i) \geq u(o(s_1, \ldots, s'_i, \ldots, s_n), \theta_i)$, where $s_i \neq s'_i$, $s_i \in S_i$ *and* $s'_i \in S_i$.

Let $s = (s_1, \ldots, s_n)$ denote the strategy profile of all agents, and the strategy of every agent except i is represented as $s_{-i} = (s, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n)$. Similarly, θ_{-i} denotes the types of all the agents except i.

A well-known solution concept in game theory is Nash equilibrium [30]

Definition A.2 *A strategy profile $s(s_1, s_2, \ldots, s_n)$ is in Nash equilibrium if no agent can switch to another strategy in favor of its own utility while keeping all others' utility non-decreasing. Thus $u(s_i(\theta_i), s_{-i}(\theta_{-i}), \theta_i) \geq u(s'_i(\theta_i), s_{-i}(\theta_{-i}), \theta_i), for\ all\ s'_i \neq s_i$.*

Please note that Nash equilibrium requires the information of other agents' strategies.

Definition A.3 *A strategy s_i is a dominant strategy for agent i if $u_i(s_i, s_{-i}, \theta_i) \geq u_i(s'_i, s_{-i}, \theta)$, for all $s'_i \neq s_i, s'_i \in S_i$.*

A dominant strategy maximizes the expected utility of agent i, no matter what strategies other agents play. Comparing to Nash equilibrium, playing dominant strategies is a more robust solution because it does not have any assumption on other agents' strategies. It is observed that in second-price sealed-bid auctions (or Vickrey auctions [31]), truth-telling is such a dominant strategy for every agent.

Mechanism design, also called *Inverse Game Theory*, is to design a set of rules of strategies and game outcomes in order to implement an optimal solution in an environment of self-interested agents which have their own preferences over different outcomes. The preference is private information only known by an individual agent. Chapter 2 in [29] gives a good review on *Classic Mechanism Design*.

Definition A.4 *A social choice function $f : \Theta_1 \times \ldots \times \Theta_n \rightarrow O$ selects the desirable outcome $f(\theta) \in O$, given a type profile $\theta = (\theta_1, \ldots, \theta_n)$.*

The goal of mechanism design is to implement a solution of the social choice function in a mechanism despite agent's self-interest.

Definition A.5 *A mechanism $\mathcal{M}$ consists of a set of strategies $\{S_1, \ldots, S_n\}$ for each agent and an outcome function $g(.) : S_1 \times \ldots \times S_n \rightarrow \mathcal{O}$, thus $\mathcal{M} = \{S_1, \ldots, S_n, g(.)\}$.*

If in a mechanism $\mathcal{M}$, there is a dominant strategy $S_i^*(\theta_i)$ for each agent i, $i = 1, \ldots, n$ and $g(S_i^*(\theta_i)) = f(\theta_i)$ for all $(\theta_1, \ldots, \theta_n) \in \Theta_1 \times \ldots \times \Theta_n$, then $\mathcal{M}$ implements the social choice function $f(.)$ and yields a desirable result. Every agent

only needs to play its dominant strategy and get a maximum expected utility without any information of others.

If the preference of an agent depends on the choice it makes in a game and the payment the choice can bring back, then the preference (or the type) can be described as a quasi-linear utility function.

Definition A.6 *A quasi-linear utility function for agent i with type θ_i is denoted as $u(o, \theta_i) = v_i(x, \theta_i) - p_i$ where x is a choice from a set of discrete choices $\mathcal{X}$, and the payment p is decided by the outcome o.*

There are two crucial properties in mechanism design: *direct-revelation* (DR) and *incentive-compatibility* (IC). In a direct-revelation mechanism the only action each agent can make is to announce its preference to the mechanism. The announced preference $\hat{\theta}_i$ is based on the true type θ_i. On the other hand, $\hat{\theta}_i$ could be either true or false. An incentive-compatible mechanism is a direct-revelation mechanism, in which agents always reveal their true types. If a mechanism implements truth-revelation (or truth-telling) as a dominant-strategy for each agent, it is *strategy-proof*. We also call a strategy-proof mechanism truthful in the reminder of this dissertation.

There is a family of successful direct-revelation and strategy-proof mechanisms, VCG mechanisms. VCG mechanisms are named after Vickrey, Clarke and Groves, who contributed to this mechanism family by their seminal papers [31, 32, 33]. VCG mechanisms are for problems, in which agents have quasi-linear preferences. According to [34], VCG mechanisms are the only direct-revelation mechanisms, which are allocation-efficient and strategy-proof.

A well-known mechanism in VCG family is the second-price sealed-bid auction, in which the best bidder wins and the winner pays the price of the second best bid. For example, there are two agents, A and B, biding for one item I, which has different

Table I. CASE ONE: AGENT A TELLS THE TRUTH

agent	value	bidding price	status	utility
A	8	8	L	0
B	10	10	W	2
A	8	8	L	0
B	10	12	W	2
A	8	8	L	0
B	10	9	W	2
A	8	8	W	0.5
B	10	7.5	L	0

values for them. Without loss of generality, suppose the value of I for A is 8, $V_A = 8$; and the value for B is 10, $V_B = 10$. Each of the agents can only bid once. The best strategy for them is bidding the true value of having I. The utility functions for A and B are

$$u_A = 8 - p$$

and

$$u_B = 10 - p$$

We show the effects of different strategies B takes in two cases. In case one, A bids its true value. In case two, A announces a value other than its type. Tables I and II illustrate the numeric results of the two scenarios. Status L denotes lost and W means win.

It is observed that only when B announces the true value of its preference, it achieves a maximum expected utility.

Table II. CASE TWO: AGENT *A* LIES

player	value	bidding price	status	utility
A	8	9	L	0
B	10	10	W	1
A	8	9	L	0
B	10	12	W	1
A	8	9	L	0
B	10	9.5	W	1
A	8	9	W	-0.5
B	10	8.5	L	0
A	8	11	W	-2
B	10	10	L	0
A	8	11	L	0
B	10	12	W	-1
A	8	11	W	-0.5
B	10	8.5	L	0
A	8	11	W	0.5
B	10	7.5	L	0
A	8	7	L	0
B	10	10	W	3
A	8	7	L	0
B	10	12	W	3
A	8	7	L	0
B	10	8.5	W	3
A	8	7	W	1.5
B	10	6.5	L	0

Let s_B denote the strategy of B telling its true value and s'_B denote any strategy as B reporting other values. Thus,

$$u(s_B, \theta_B) \geq u(s'_B, \theta_B), s \neq s'$$

VCG mechanisms are a family of efficient, and strategy-proof direct-revelation mechanisms on quasi-linear preference. A quasi-linear utility function consists of two parts, like

$$u_i(k, p_i, \theta_i) = v_i(k, \theta_i) - p_i$$

where $v_i(.)$ is the value function of agent i and p_i is its payment.

We let $g(\hat{\theta})$ be the outcome function in terms of a choice function, $k : \Theta_1 \times \ldots \times \Theta_n \rightarrow \mathcal{K}$, and a payment function, $t_i : \Theta_1 \times \ldots \times \Theta_n \rightarrow \mathcal{R}$, for each agent.

In VCG mechanisms, the outcome function $g(\hat{\theta})$ always decides on a choice k^* that maximizes the total value. It computes:

$$k^* = arg \max_{k \in K} \sum_i v_i(k, \hat{\theta}_i) \tag{2.1}$$

Then, given a profile of the reported types $\hat{\theta} = (\hat{\theta_1}, \ldots, \hat{\theta_n})$, the payment function of VCG mechanisms is defined as

$$t_i(\hat{\theta}) = h_i(\hat{\theta}_{-i}) - \sum_{j \neq i} v_j(k^*, \hat{\theta}_j) \tag{2.2}$$

where $h_i : \Theta_i \rightarrow \mathcal{R}$ is an arbitrary function over the reported types of all agents except i. The variety on the selection of function $h_i(.)$ produces the diversity of VCG mechanism family.

The utility of an agent i in the VCG is:

$$u_i(\hat{\theta}_i) = v_i(k^*(\hat{\theta}), \theta_i) - t_i(\hat{\theta}) \tag{2.3}$$

$$= v_i(k^*(\hat{\theta}), \theta_i) + \sum_{j \neq i} v_j(k^*(\hat{\theta}), \hat{\theta}_j) - h_i(\hat{\theta}_{-i}) \tag{2.4}$$

Ignoring the $h_i(\hat{\theta}_{-i})$, which is independent of i's reported value, the goal of agent i is to solve:

$$\max \left[v_i(k^*(\hat{\theta}_i), \theta_i) + \sum_{j \neq i} v_j(k^*(\hat{\theta}_j), \hat{\theta}_j) \right] \tag{2.5}$$

As in choice function (2.1),

$$k^* = arg \max_{k \in K} \sum_i v_i(k, \hat{\theta}_i) \tag{2.6}$$

$$= arg \max_{k \in K} \left[v_i(k, \hat{\theta}_i) + \sum_{j \neq i} v_j(k, \hat{\theta}_j) \right] \tag{2.7}$$

Only when i reports its true value, will the mechanism and i have tuned value functions to compute. In that case, function (2.7) assures to solve (2.5) so that it maximizes the result of agent i's utility function (2.4), whatever other agents' reported values.

As incentive-compatible (IC) mechanisms, VCG mechanisms align the utility functions of individual agents with the goal of a system. Therefore if an agent tells the truth, the system guarantees to best serve its interests.

VCG mechanisms are able to prevent any single cheater, but cannot achieve strategy-proofness if collusions can happen.

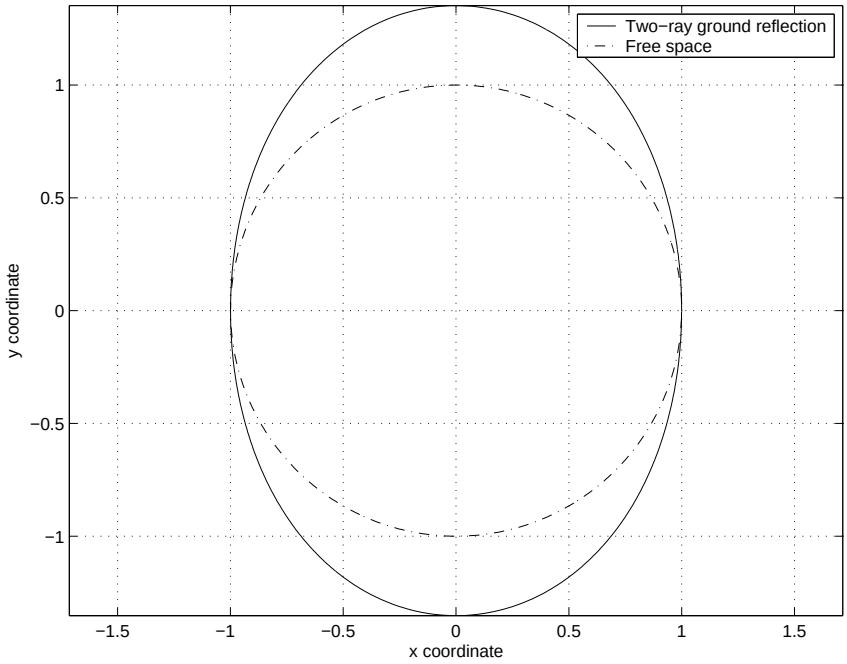


Fig. 1. Power efficient relay area of free space model and two-ray ground reflection model. When a sending node S is at (-1, 0) and a receiving node R is at (1, 0), a route passing through an intermediate node in the enclosed area consumes no greater total transmission power than the direct path from S to R.

B. Radio Propagation Models

Due to the characteristics of radio channel propagation models, transferring a packet may cost less power if it is relayed by multiple intermediate nodes rather than transferred over a single long-distance hop. In the two-ray ground reflection model, the power of received signal Pr is expressed as the formula below [35].

$$P_r = \frac{P_t \times G_t \times G_r \times (H_t^2 \times H_r^2)}{d^4} \tag{2.8}$$

In (2.8), d is the distance from the transmitter to the receiver; P_t is the emission power at the transmitter; G_t and G_r are transmitter and receiver's antenna gains; H_t and H_r are the height of the antennas.

The received power is inversely proportional to d^4. If the distance decreases by a half then the transmission power can reduce to the $\frac{1}{16}$ of the original value while keeping the same P_r. Reducing transmission power can decrease radio interference and increase network lifetime.

If we use k to represent the constant factors in the formula above, then for the two-ray ground reflection model we have:

$$P_r = \frac{P_t \times k}{d^4} \tag{2.9}$$

There is a threshold for the received signal strength P_r. If P_r is greater than or equal to a threshold P_{rthd}, the packet is received successfully. Otherwise, the receiver cannot interpret the packet.

Obviously, with this P_{rthd}, the minimal transmission power, P_{tmin}, used by a sender is:

$$P_{tmin} = \frac{P_{rthd} \times P_t}{P_r} \tag{2.10}$$

Hence, a node is able to compute the minimal emission power P_{tmin} to reach another node as long as the receiver measures the received signal strength and reports the value to the transmitter.

Using α to denote a general exponent of d and K to represent all the constants, we have:

$$P_{tmin} = K \times d^{\alpha},\ \alpha \in [2, 6] \tag{2.11}$$

In the free space radio propagation model, α equals 2. And α equals 4 for the two-ray ground reflection model.

Receiving packets also incurs power consumption. Comparing to the transmission power, the receiving power is small [36]. To simplify the analysis, we ignore the

receiving power in this dissertation as well as the power consumption on signaling messages.

Fig. 1 shows the area in which if there is a node to forward packets for a pair of nodes at coordinate $(-1, 0)$ and $(1, 0)$ respectively, then the two-hop path requires less total transmission power than a direct transmission.

C. System Model

A wireless ad hoc network can be interpreted as a weighted graph, $G(V, E, W)$. Network nodes are represented by a set of vertexes V. If node u is within the communication range of node v, there is an edge (u, v) between them. We assume all nodes are identical and all links are bi-directional. The cost $W_{u,v}$ on edge (u, v) is the transmission power $P_{u,v}$ consumed on the sender side.

We denote a source node as S, which generates and sends out packets, and a destination node as D. S is the start of a path while D is the end. A path from S to D is a series of node identifiers, $\sigma_{S,D} = \{S = \sigma_0, \sigma_1, \ldots, D = \sigma_L\}$. L is the number of hops along the path. $d_{u,v}$ is the Euclidean distance between node u and v.

In a routing protocol, we demand each node to advertise its transmission power in its packets. The receivers will measure the received signal strength and report the calculated minimum emission power to the sender. Hence the sender can adjust its sending power level accordingly.

However, due to the irregularity of the radio propagation in the real environment, the ideal minimum transmission power is hard to get if not nonexistent. Then, in a real application, this may be implemented as different emission power levels at the sender side. A sender can choose a transmission power level based on the feedback from the receiver to achieve better channel quality while saving energy. To simplify

the analysis, we still use the minimum transmission power in later sections.

So the weight of a path from S to D can be expressed as

$$W_{S,D} = \sum_{i=0}^{L-1} P_{\sigma_i,\sigma_{i+1}} = K \sum_{i=0}^{L-1} d^{\alpha}_{\sigma_i,\sigma_{i+1}}$$

Definition C.1 *A Minimum Transmission Power (MTP) path is a path from its source S to its destination D, along which the total transmission power P_{MTP} is not greater than any other path connecting the same pair of nodes.*

We do not demand any positioning services in a network. A node does not have to know any geographical information. However, every node needs to be able to detect the direction, from which a packet is received. Using directional antenna technology, this is achievable.

To encourage collaborations among network nodes in MANETs, we use monetary transfers to create cooperative incentives in a, otherwise, non-cooperative environment. We claim there is some virtual currency system, like Nuglets [20], in the MANETs we conduct our investigations.

There should be a relationship between one unit of payment and one unit of energy (or power). In this dissertation, we do not give a method to decide the value of a payment unit. But we believe one unit of virtual money used for paying network nodes should be able to trade one unit of energy (or power).

For the truthful routing in MANETs (Chapter III), we assume that a secure payment facility exists in ad hoc networks. Some peer works, like Sprite [37], provide appropriate evidences for this assumption. If a node promises to forward network packets, its payment will be determined by the routing protocol. The payment facility assures to deliver the payment by the right amount securely after a node has really served.

There is a finance center (FC), like the Credit Clearance Service (CCS) in [37], which has an authority to draw a tax from each node and use it to pay service providers for the public welfare. When a node has a link to the finance center, the debit and credit transactions will be performed. A source is assumed to be truthful because it needs the network service to fulfill its own tasks.

The FC can even work off-line while the serving nodes move to it and bring evidences of services to claim their payment. For example, a school can implement the finance center because it is easy for it to collect service fees and spend them for good. We also assume there is no collusion among network nodes and the control messages are forwarded by each node for free. Every node can be given a certain amount of initial funding to pay the tax and the communication fees.

CHAPTER III

TRUTHFUL ROUTING IN MANETS

A. Introduction and Motivation

Limited resource possession is the main motivation for a node to be selfish. Mobile devices, such as laptops and PDAs, are battery powered. The energy reserve is limited and cannot be quickly replenished. Therefore they always intend to save energy for themselves. We can see as long as network nodes are managed by individual authorities, which are only interested in their own welfare, selfishness is inevitable.

On the other hand, node cooperation is the basis of network services. Serving for the network functions should not come for free. As the service providers get compensation in some form for their cost, the intention of cooperating with others is stimulated.

Game theory [27], in particular, mechanism design gives us a powerful tool to model cooperative and non-cooperative interactions between different agents. In a game, an agent has its own preference, called type, which is represented by a utility function. The type is private information unknown to other agents. A rational agent has the incentive to maximize its utility while playing a game. In the game theoretic setting, the network nodes act as the agents in a game.

A truthful mechanism induces, instead of forcing, network nodes to tell truth and collaborate with each other. We study the effect of mechanism design on routing and forwarding in MANETs. We believe any routing algorithm needs to take the selfishness into account, otherwise its performance cannot be assured when dealing with self-interest oriented MANETs.

We propose a truthful routing protocol - Transmission power rEcursive Auction

Mechanism (TEAM) protocol for MANETs. With TEAM, we call for auctions in the route discovery process and design appropriate payment function to cope with selfish behaviors.

B. Prior Arts

PARO [2] reduces the aggregate transmission power by taking advantage of multi-hop transmission. It allows a route to be redirected by intermediate nodes. Since the nodes in ad hoc networks have the intention to be selfish, they may not volunteer to redirect a path all the time. SPAN [1] elects coordinators to form a forwarding backbone. Non-coordinators can enter the doze state to save energy. SPAN does not use adaptive emission power, thus every node keeps a uniform power level as long as it is on. This may cost more energy than necessary and cause more radio interference.

GAF [7] divides an area into virtual grids. Nodes in the same grid are the equivalent routers. They shift in three states: active, sleeping and discovering so that they can forward network traffic in turn. Li, et al. [14] study the relationship between the transmission range and the connectivity of resulted graphs. They show that (K+1)-connected graph can be achieved with certain probability when the emission radius and the node number satisfy some conditions.

In [38], Dorsey calls the protocols, which ignore the fact that a node is willing to save energy for its own usage, compulsory protocols. In real world, a protocol may not have the authority to force all nodes to do what they are supposed to do. In contrast, individual nodes in ad hoc networks are able to manipulate a protocol. Marti, et al. [16] show that even a small portion of misbehaving nodes can degrade the network performance dramatically. [17, 18] attack security routing by establishing countermeasure mechanisms against malicious nodes. However, selfish nodes are

different from malicious nodes because they are rational.

Economic concepts have already been introduced into distributed system research area [39]. In [20, 21, 38], the collaborations between different nodes are no longer taken for granted. Instead, some mechanisms are designed to stimulate the cooperative works. In [20], network services are traded on each hop toward the destination.

Viewing and solving problems in distributed systems from the perspective of mechanism design is a recent trend [40, 41]. Nisan and Ronen [42] discusses mechanism design and its applications from the algorithmic aspect. Ad hoc-VCG [22] is a work close to our research. It implements a generalized VCG mechanism in ad hoc networks in order to achieve the cost-efficiency and truthfulness. It pays intermediate nodes a premium, which covers the incurred cost. Its payment assures the Individual Rationality (IC) and the overpayment has a theoretical bound. However the message overhead of Ad hoc-VCG is high, $O(n^3)$, in that it exhausts each possible path to find the most energy efficient. TEAM [23] improves the power efficiency along a path while keeping the message complexity low at $O(n+L\times n)$ and achieving truthfulness.

C. Truthful Routing Protocol Design for MANETs

1. TEAM Protocol Design

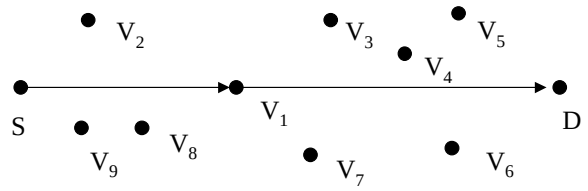
The intuition of TEAM is that it may not find the most energy efficient path, a MTP path, but through a truthful mechanism it can find an alternative, which approximates the MTP path. We divide the route discovery into two phases. First, TEAM runs an AODV-like protocol [43] to find a minimum-hop route from the source S to the destination D. Initially, S broadcast a route request RREQ into the network. Each node receiving the RREQ checks whether it is the destination. If it is not, it forwards the request by broadcasting it again. After the destination node receives the RREQ,

a route reply message RREP is created and sent out along the backward path. Each node on the route records the destination node and next hop toward it. As soon as the source receives the RREP, a minimum-hop path is established and phase two starts.

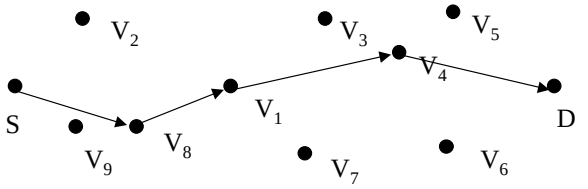
Since the energy efficiency along a route is improved in phase two, the longer each hop in phase one, the bigger improving space we have in phase two. The RREQs need to be broadcast with maximum power by each intermediate node. To induce nodes to broadcast in this way, TEAM makes the price of each communication session flat at M, which is the amount a source needs to pay. All the nodes, chosen in phase one, share the payment. Thus, each node will receive $\frac{M}{L-1}$ equally, while L is the hop count of the path. Only when L decreases, can intermediate nodes increase their payoffs. The value of M is based on the diameter of a network. We just assume this value is decided beforehand in a way to make it attractive enough for any forwarding nodes and affordable for any source nodes.

In phase two, TEAM calls for auctions within each hop on the current path. The nodes picked in phase one have known their payoffs that will not change no matter what phase two turns out. Thus these nodes will act correctly in phase two. In addition, security monitoring methods, such as the Watchdog [16], can be applied into the network to ensure behavior. Since we assume there is no collusion among selfish nodes, it is reasonable to believe that a rational node does not want to take the risk of losing its secured payoff.

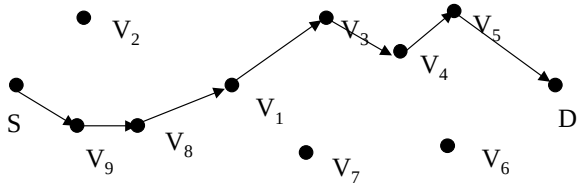
Intermediate nodes, which are overhearing the routing messages and within the communication range of both the upstream and downstream nodes, v_i and v_{i+1}, bid to redirect the path as long as the redirections can reduce power consumption. Each of those intermediate nodes uses one-hop broadcast messages, as the Hello messages, to announce the total transmission power spent along a redirected path that goes



(a)



(b)



(c)

Fig. 2. Route discovery: establish a path through recursive auctions.

through it. The cost of a redirecting node is its transmission power for forwarding packets to its successor. If it reports correctly, the cost cannot be greater than its announced value. Since we have assumed there is a relationship between payment and power, we just use them interchangeably.

The best bid, or the minimum transmission power redirected path, wins the auction. The two end nodes of the hop update their routing tables according to the auction result. The winner receives a payoff, Pf, which is equal to the second best bid. By the design of TEAM, the second best bid is the transmission power on another path from v_i to v_{i+1}. This value can cover the cost of the winner (redirector), if it has reported correctly.

Since each node has a maximum emission power level, and its participation is voluntary, the cost cannot be arbitrarily high. The finance center draws taxes from each node to pay for the public affairs. This is reasonable because the network-wide energy saving is beneficial for each node.

Then,

$$Pf_{v_j} = \hat{P}_{v_i,v_k} + \hat{P}_{v_k,v_{i+1}} \tag{3.1}$$

v_j is the winner of an auction and v_k is the node of the second best bid. .

After a redirection ends, another round of auctions starts within the newly redirected hops as long as a power improvement can be achieved. Fig. 2. depicts how a path is recursively redirected. Please note that in a real-world application, the auction stop condition may be modified in order to take the receiving energy consumption into account. But in the following sections we just keep ignoring it to simplify the analysis. Since the new auctions do not change the payoff of redirectors selected previously, these nodes have no intention to misbehave from now on.

TEAM does not establish the final path at once. Intermediate nodes are put into the cooperative situation one by one through each auction. The advantage of recursive auctions is that we can prevent cheating in each round. As a node is picked by the protocol, it secures its payoff by working correctly. Afterwards, it does not need to lie anymore. This mechanism stimulates cooperation in an environment where the selfish behavior is almost certain.

2. Truthfulness Analysis of TEAM

The only goal of a rational node is to maximize its utility. So the utility function decides the behavior of the a rational node.

In TEAM, a redirector v_j has a utility function as:

$$u_{v_j}(\hat{\theta}_{v_j}) = -c_{v_j}(o(\hat{\theta}), \theta_{v_j} + m_{v_j}(o(\hat{\theta})) \tag{3.2}$$

In (3.2), c_{v_j} is the cost function of v_j. m_{v_j} is its payoff. o is the outcome of a mechanism based on all the announcements $\hat{\theta}$. The mechanism guarantees a non-negative utility to every participant if it declares truthfully.

The utility function (3.2) is comprised of two parts. One is the cost of cooperation; another is the payoff. The real cost θ is the private information of each node, so it is unknown to all the other nodes. TEAM mechanism is a direct revelation mechanism, which demands each node to announce its cost and decide the payoff based on the received announcements. The auctioneers in each round are the bidders of the previous round. TEAM decides the payoff to a redirector by using the second-price sealed-bid auctions, which is a subset of the VCG mechanism family. Therefore, TEAM follows the truthfulness of VCG mechanisms immediately.

As we mentioned above, a sender includes the transmission power in its packets.

A receiver calculates and reports the minimum power needed by the sender to reach it. As an overhearing node v_j competes to be the redirector within a hop, it needs to report to upstream node, v_i, the minimum power $P_{v_i,vj}$ and listen to the downstream node, v_{i+1}, to get the minimum power $P_{v_j,vi+1}$. Since the payoff for a redirector is equal to the second best bid, v_j cannot cheat to increase its earning.

v_j has three strategies to report P_{v_i,v_j} and $P_{v_j,v_{i+1}}$: overstating , understating or reporting the true value.

Theorem C.1 *TEAM protocol is strategy-proof.*

Proof First, v_j tells the true value of the power used by v_i. It is because if it gives a higher value, it may not be selected as a redirector so that it cannot earn the payoff. If it is still chosen, it's payoff does not change because the protocol pays whatever the second best bidder, without loss of generality, say node v_k, reports. If it sends a lower power value, the communication may fail, which causes it to lose the payoff. Therefore, v_j always tells the truth to the upstream node v_i.

Second, v_j always announces its transmission power correctly. If it exaggerates its emission power value, the downstream v_{i+1} will reply with a higher value. That may cause v_j to lose the competition with others. Suppose it is still selected then its payoff is the same as it announces a true value. To prevent a false decreased emission power value, we let v_{i+1} do a handshake with v_j with the calculated minimum power. If it fails, then v_{i+1} informs v_i. v_j will be kicked out because it does not announce correctly. As a result, if an intermediate node v_j wants to be the redirector, it has to act truthfully.

The values of node v_j's utility function in different cases are shown as (3.3). In (3.3), v_k is the second best bidder; $\theta_{v_j}, \hat{\theta}_{v_j}, \hat{\theta}_{v_k}$ are the true value of v_j, the announced value of v_j and the announced value of v_k respectively.

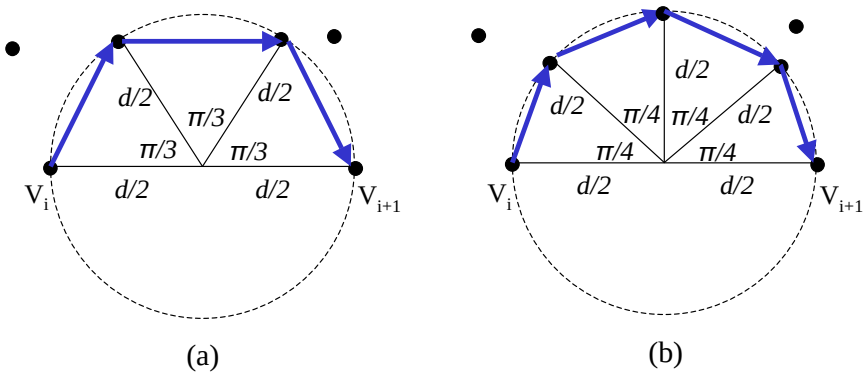


Fig. 3. There is no redirector in the circle with the diameter d. However, there exists an MTP path. (a)L=3 (b)L=4

$$u_{v_j}(\hat{\theta}_{v_j}) = \begin{cases} -P_{v_j,v_{i+1}} + \hat{\theta}_{v_k} & \hat{\theta}_{v_k} > \hat{\theta}_{v_j} = \theta_{v_j} \\ -P_{v_j,v_{i+1}} + \hat{\theta}_{v_k} & \hat{\theta}_{v_k} > \hat{\theta}_{v_j} > \theta_{v_j} \\ 0 & \hat{\theta}_{v_j} > \hat{\theta}_{v_k} > \theta_{v_j} \\ 0 & \hat{\theta}_{v_k} > \theta_{v_j} > \hat{\theta}_{v_j} \end{cases} \tag{3.3}$$

When the winner secures its payment, which guarantees to cover its cost, it does not have to cheat. Thereafter, with the integration of some network monitoring technology, the system assures all the nodes stay as truth-tellers. Therefore, any node cannot act strategically to take advantage of the network.

3. Efficiency Analysis of TEAM

Intuitively, TEAM can save power along a multi-hop path. In this section we show that if the source S and the destination D can communicate directly in one hop with maximum transmission power, the total power of a TEAM path can be bounded within $\lceil \frac{L}{2} \rceil P_{MTP}$, where L is the hop number of the MTP path.

From the protocol design, we know if an intermediate node, v_j, wants to be a redirector, the path passing through it must consume less power than the direct transmission from the upstream node, v_i, to the downstream node, v_{i+1}. We use the free space radio propagation model [35] in our analysis. Consequently the first redirector must be in a circle area with diameter $d_{v_i,v_{i+1}}$, which is the Euclidean distance from v_i to v_{i+1}. If there is no such node inside the circle area, TEAM always prefers a direct transmission. We study TEAM in two cases. One is that there is no redirector found. The other is that there is at least one redirector chosen by the protocol.

In the first case (see Fig. 3.), if there is a MTP path from v_i to v_{i+1}, different than the direct path, it must circumvent the circle to reach v_{i+1}. If the MTP has a length L, the power spent along it cannot be less than the path that $L-1$ nodes are evenly distributed on a half circle from v_i to v_{i+1}. We denote the aggregate transmission power on the MTP path with L hops as P^L_{MTP} and that on the ideal path as P^L_{min}, then we have

$$P^L_{MTP} \geq P^L_{min}$$

$$P^L_{min} = L\frac{P_{thd}}{K}[(\frac{d^2}{2}) - \frac{d^2}{2}cos(\frac{\pi}{L})] = L\frac{P_{thd}}{K}\frac{d^2}{2}[1 - cos(\frac{\pi}{L})]$$

$$P^L_{MTP} \geq L\frac{P_{thd}}{K}\frac{d^2}{2}[1 - cos(\frac{\pi}{L})] \tag{3.4}$$

As we know,

$$P_{TEAM} = \frac{P_{thd}d^2}{K}$$

By substitution,

$$P_{TEAM} \leq \frac{2}{L(1 - cos(\frac{\pi}{L}))}P^L_{MTP} \tag{3.5}$$

When

$$L = 3, \quad P_{TEAM} \leq 1.33 P_{MTP}$$

$$L = 4, \quad P_{TEAM} \leq 1.71 P_{MTP}$$

$$L = 5, \quad P_{TEAM} \leq 2.09 P_{MTP}$$

$$L = 6, \quad P_{TEAM} \leq 2.49 P_{MTP}$$

$$L = 7, \quad P_{TEAM} \leq 2.89 P_{MTP}$$

$$\ldots$$

Now we study the second case in which at least one redirector is found inside the circle. Because of the design of TEAM and wireless propagation characteristics, the first redirector is always the node nearest to the middle point of a straight line from v_i to v_{i+1}. If it is also the middle point on the MTP path which has a length L, then

$$P_{TEAM} \leq \lceil \frac{L}{2} \rceil P_{MTP} \tag{3.6}$$

In Fig. 4., the MTP path from v_i to $v_{i+1}$is $\{v_i, v_i^0, v_i^1, v_i^2, v_{i+1}\}$. v_i^1 is the first redirector selected by TEAM. $d_{v_i V i^1}$, $d_{v_i^1 v_{i+1}}$ denote the distances from v_i to v_i^1 and from v_i^1 to v_{i+1}. So,

$$P_{TEAM} \leq \frac{P_{thd}}{K}(d^2_{v_i V i^1} + d^2_{v_i^1 v_{i+1}})$$

Since there are two hops before and after v_i^1, then

$$P_{MTP} \geq \frac{P_{thd}}{K} \frac{d^2_{v_i v_i^1} + d^2_{v_i^1 v_{i+1}}}{2}$$

Thus, we have

$$P_{TEAM} \leq 2 P_{MTP} \tag{3.7}$$

The length of MTP is 4 in Fig. 4., so (3.6) is true. Actually in this simple topol-

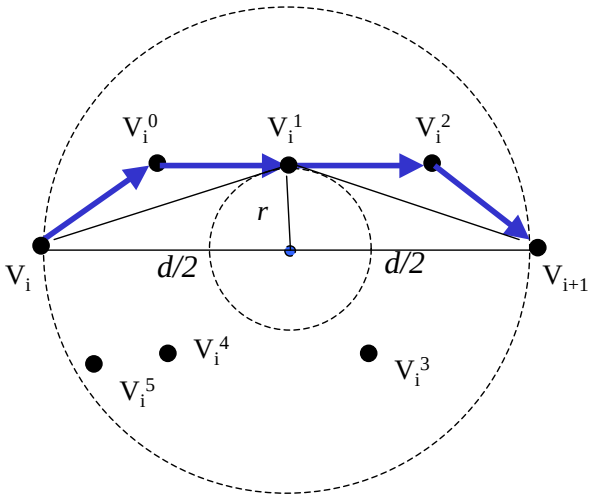


Fig. 4. There is a TEAM path in the circle with diameter d. The first redirector is the middle point of the MTP path.

ogy, the two intermediate nodes, v_i^0 and v_i^2, will also be chosen by TEAM recursively. It is not surprising to see that TEAM finds a path, which is also a MTP path.

Furthermore we prove that the bound (3.6) is held even when the first redirector is not on the MTP path. For instance, in Fig. 5., the MTP path is $\{v_i, v_i^0, v_i^1, v_i^2, v_{i+1}\}$. We choose the node in the middle of the path, which is v_i^1 in this topology. Since the v_{TEAM}^0 is the winner of the first auction, the 2-hop path passing through it consumes less transmission power than any other 2-hop path from v_i to v_{i+1}. So we have

$$(d_{v_i v_{TEAM}^0})^2 + (d_{v_{TEAM}^0 v_{i+1}})^2 \leq (d_{v_i V i^1})^2 + (d_{v_i^1 v_{i+1}})^2$$

(3.6) is still true in Fig. 5. When we substitute v_i with S and v_{i+1} with D, $\lceil \frac{L}{2} \rceil P_{MTP}$ is the bound of the power efficiency of the TEAM path if S can contact D directly. We can expect much better performance of TEAM since it is rarely to see that TEAM just finds a single redirector while the MTP path has multiple hops. With the increase of node density, there are more alternative paths from S to D. TEAM finds an approximately optimal path among those alternatives. Along the

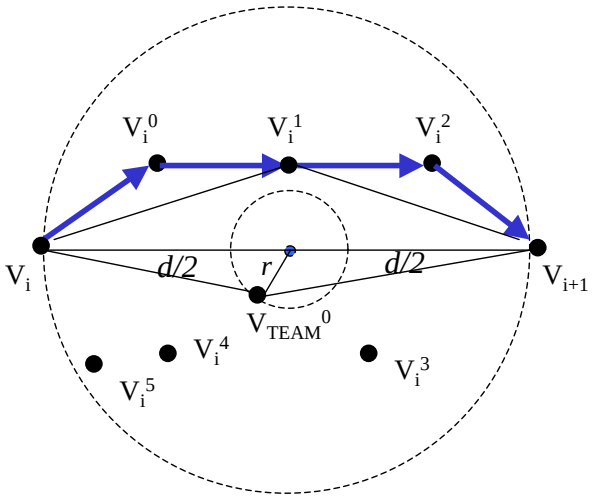


Fig. 5. There is a TEAM path in the circle with diameter d. The first redirector is not on the MTP path.

TEAM path, every node is willing to forward network packets and earn its payoff.

Inherited from AODV, the message complexity of TEAM is $O(n)$ in phase one. In phase two, TEAM calls for the power auctions recursively. The nodes on the final path are picked one by one, resulting in $O(L \times n)$ messages in a stationary network. L can be the diameter of a graph or, in the worst case, n. Please note that all nodes only need to broadcast the control messages at full power level in phase one. During the auctions, they can reduce their transmission power to a lower level, which is enough to negotiate with neighbors. This is a desirable property because the radio interferences can be reduced and so is the energy consumed on control messages. In Ad hoc-VCG[22], cost efficiency is assured with a high message overhead, $O(n^3)$. Comparing to that, TEAM achieves power efficiency with a significantly lower message overhead.

D. Simulation of TEAM and Results

In order to investigate the performance of TEAM in term of power efficiency, we simulate TEAM in ns-2 network simulator [44] with the wireless extension of Monarch

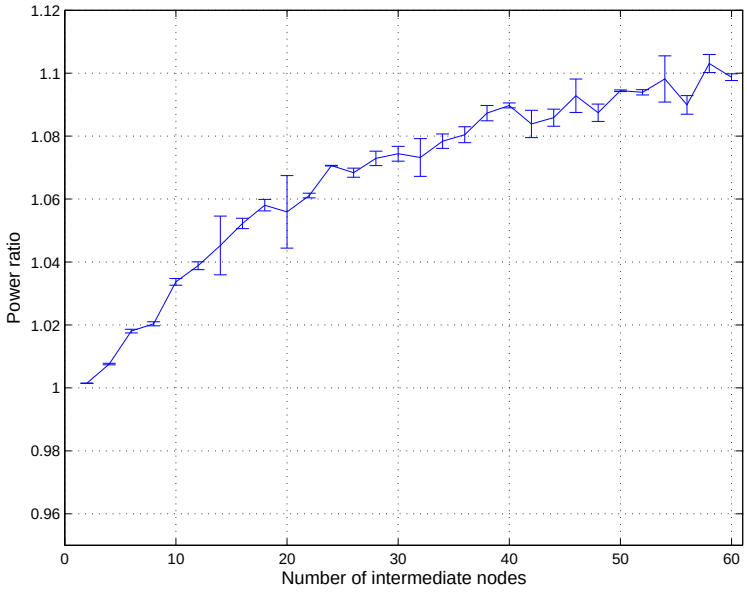


Fig. 6. The average ratio of the power on a TEAM path vs. a MTP path at different node densities.

project [45]. TEAM runs as a routing protocol on the top of IEEE 802.11 MAC layer, which uses Carrier Sense Multiple Access with Collision Avoidance technique (CSMA/CA). Before the data transmission, RTS-CTS are exchanged between the sender and receiver. The data packets are transmitted using dynamic minimum power, while RTS and CTS are always sent with maximum transmission power.

Every node in our simulations has radio with 2Mbps bandwidth and 250-meter communication range. We run TEAM in a 300m $\times$ 300m area, in which we vary the node number from 2 to 60. Nodes are stationary and put in the area randomly with a uniform distribution. Because in phase one all nodes broadcast at the maximum power, the distance between a pair of adjacent nodes on a phase one path is usually the same as the maximum communication range. We put a pair of nodes on the different sides of the network area as the source and destination. In each topology

the source initiates a route discovery by sending out a RREQ. After two phases, a power efficient path is established. The aggregate transmission power is measured. We repeat the experiment 1000 times for each node density.

We also implement the Dijkstra algorithm to find the MTP paths in the same network topologies as TEAM. The power efficiency ratio, which is the aggregate transmission power of a TEAM path against its MTP counterpart, is plotted in Fig. 6. The experiment data is listed in Table VI in Appendix B.

It is observed that with the increase of node density, the power efficiency ratio increases. It means that the TEAM paths shift away farther from the MTP paths. This is because the more nodes around, the more alternative paths from the source to the destination. Though TEAM tries to optimize the power efficiency greedily in each round of phase two auctions, the final result may not be the best. However it is shown the performance of TEAM is close to the optimal result since the ratio only increases within a narrow range even when the network topology becomes pretty dense (e.g. 60 nodes within the simulation area). TEAM can almost find the MTP path for sure when the network is very sparse.

E. Summary

In wireless ad hoc networks, cooperation among profit-oriented nodes cannot be taken for granted anymore. Each node is free to follow its own interests. Although researchers have proposed a wealth of energy saving protocols, the selfishness in ad hoc networks has not been noticed until recently.

Selfish nodes are different from malicious nodes. A selfish node is rational and not interested in attacking other nodes. Its objective is to maximize its own profit. Researchers have shown that even a small part of misbehaving nodes can degrade

the network performance dramatically. Inducing selfish nodes to cooperate by using payment is a promising approach to tackle the selfishness problem in MANETs. Game theory, in general, mechanism design, in particular, seems to be the appropriate tool to cope with interest conflicts.

In this section, we present the Transmission power rEcursive Auction Mechanism (TEAM) routing protocol to discover a power efficient path, which approximates the Minimum Transmission Power (MTP) path, in an ad hoc network that consists of selfish nodes. TEAM pays the service providers according to their contributions. Recursive auction routing can induce nodes to cooperate with each other and significantly reduce the message overhead comparing to Ad hoc-VCG. Each node decides whether to participate the routing service voluntarily in TEAM.

We prove that with an underlying secure payment facility, TEAM is truthful. No node can lie without decreasing its payoff. If the source and destination can communicate with each other directly, the performance of TEAM has a theoretical bound.

CHAPTER IV

TRUTHFUL TOPOLOGY CONTROL IN MANETS

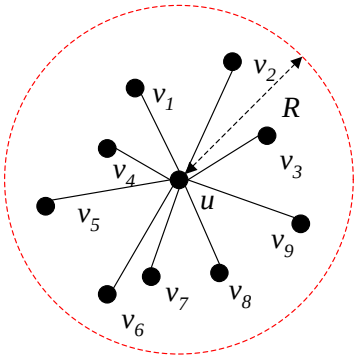
A. Introduction and Motivation

Topology control technology let network nodes in a MANET adjust their transmission power in order to reduce their neighbor sets. Fig. 7. shows the topology changes as a node uses different transmission power. When every node transmits using its maximum power, the network graph is denoted as $G(V, E)$. The graph derived by topology control is $G'(V, E')$, which is a subgraph of $G(V, E)$, $G'(V, E') \subseteq G(V, E)$. G' must preserve the connectivity of G. In other words, if a pair of nodes u and v is connected in G, they should be connected in G' too.

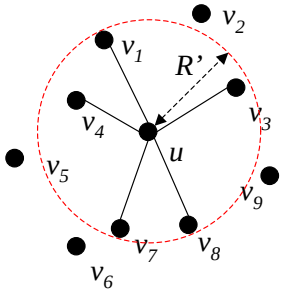
In G', the node degree is lower than in G so that a node is expected to have less neighbors than in G. This is desirable in MANETs because the short the edges, the less power a node uses to transmit and the smaller area the radio interference can influence. Furthermore, the wireless network capacity is closely related to the node degree. The network throughput drops quickly as the network size increases [46, 47]. Comparing the power-efficient routing, topology control is a pro-active method to reduce power consumption and radio interference.

All the topology control algorithms assume that network nodes cooperate with each other. Forming a power efficient network topology without degrading the network connectivity needs the collaborations among all the nodes. No existing topology control techniques can success without any interaction between different network nodes.

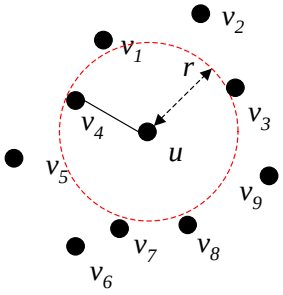
However, as we discuss in previous chapters, in a MANET the selfish behaviors are inevitable because of the lack of system regulation power and the resource scarcity.



(a)



(b)



(c)

Fig. 7. When node u uses different transmission power, its neighbor set changes. In (a), u transmits with the maximum power. Its communication radius is R. In (b), u reduces the power and has a radius R' ($R' < R$). As u sets its communication range as r ($r < R' < R$), it can only communicate with the nearest neighbor v_4.

Rather than ignore the selfish intention, we design a truthful topology control mechanism, TRUECON, to stimulate cooperation in order to discover a resource-efficient network topology.

B. Related Work

Rodoplu and Meng [8] present a distributed algorithm to reduce the transmission power of each node, while maintaining the minimum energy paths. Li and Halpern improve the algorithm in [8] by proposing SMECN (small minimum-energy communication network) [9]. They define a type of edges, 2-redundant edges in term of power consumption. They claim SMECN preserve the network connectivity and eliminate all 2-redundant edges. Comparing to Rodoplu and Meng's algorithm, SMECN terminates faster and achieves the same result. Both of the algorithms need the aid of some positioning service, such as GPS. In [11], Ramanathan and Rosales-Hain present a spanning tree algorithm to achieve connected static networks.

In [10, 48], Wattenhofer et al. propose Cone-based Topology Control algorithm (CBTC), in which a node only needs to know the direction of its neighbors and the transmission power to reach them. They show that the algorithm can approximate the optimal solution arbitrarily when the parameter is carefully selected. In CBTC, a node reduces its transmission power to form a smaller neighborhood than using its maximum transmission power. They prove that if in each cone not greater than $\frac{5\pi}{6}$, there is at least one neighbor for a node, the derived network graph preserve the connectivity of the original graph. They give three strategies to optimize the algorithm so that the node degree in the final graph can be further reduced. We base our truthful topology control algorithm on CBTC. However, we prove that our algorithm achieves, in MANETs, a crucial property, which CBTC cannot assure,

truthfulness.

Li et al. [14] study the topology control from the perspective of fault tolerance. They show that (K+1)-connected graph can be achieved with certain probability when the transmission radius and the node number satisfy certain conditions.

[46, 47] show, theoretically and practically, the network throughput is expected to be $O(\frac{1}{\sqrt{n}})$, n is the number of nodes in a network. As a result, while a network size grows, the throughput keeps dropping. Their works also validate the importance of topology control technology. If the node degree does not increase as the growth of the network size, we may expect the network throughput not to fall dramatically.

Another type of topology control technology works on the MAC layer protocol. Cerpa and Estrin design ASCENT [12], an self-configuring topology control protocol for sensor networks. ARCENT adaptively elects a few active nodes for the whole network. The selection of active nodes is based on various parameters, including neighbor threshold and packet loss rate, etc. Non-active nodes can turn off their radio for a period and wake up after a sleep timer expires.

PAMAS [13] takes advantage of overhearing. Due to the broadcast characteristic of radio propagation, a node can overhear the packets, which are not destined to it. If an overhearing node senses the communication of other nodes and knows it cannot transmit any packet for a while, it turns off its radio component to save energy.

Among these algorithms, every network node is assumed to collaborate with others all the time. In another word, the incentive of a node is ignored. If there is no attraction of the cooperation, we cannot expect the network can function well. For example, Li et al. [48] have proved that a cone of $\frac{5\pi}{6}$ is the tight bound of preserving the network connectivity while reducing the connection degree. So the minimum number of a node's neighbor is 3. If a node u establish such a neighbor set with node v, w, x, each neighbor is critical for u. Without loss of generality, v wants to save

its energy and stops forwarding packets for u. u may either suffer from an isolation from the other part of the network or have to increase its power to discover another neighbor which can replace v. In either way, the topology control scheme is defeated by the selfish intention.

In [24], Eidenbenz et al. propose a truthful routing protocol COMMIT to cope with selfish nodes in MANETs. COMMIT prevent a source node from utilizing strategies and achieve a budget control along a power efficient path. However it relies on a topology control algorithm to restrict the node degree beforehand. If we cannot trust selfish nodes in routing, can we trust them at other stage? The answer must be **No**. As a result, truthful mechanisms are needed at any time when selfish nodes interact with each other.

C. Truthful Topology Control - Topology Control in Non-Cooperative Environment

A Truthful Topology Control (TTC) mechanism needs to induce nodes to reveal their true costs and find the optimal solution for network resource management based on the announced values. Designing a mechanism, in which truthful-telling is the only dominant strategy, is the goal of Truthful Topology Control.

We present Truthful topology Control algorithm (TRUECON) based on VCG mechanisms. To the best of our knowledge, this is the first research to consider topology control in a non-cooperative environment.

1. TRUECON - a Truthful Topology Control Algorithm

Like CBTC[10], TRUECON needs to know the direction, from which a message is received. The direction information can be obtained by using directional antennas. The communication area of a node is modeled as a Unit Disk Graph(UDG). A node

u periodically broadcast *Hello* messages, in which it put its current sending power value P_s. Upon receiving a *Hello* message, a node v_i measures the received signal strength P_{r_i} and calculates the minimum power P_{u,v_i} needed by u to reach it. Node v_i then replies with an *Ack* packet, in which it declares P_{u,v_i} as $\hat{P}_{u,v_i}$. $\hat{P}_{u,v_i}$ may not be equal to P_{u,v_i}. Node u would decide the price of its neighbors based on the announced values. If u uses one of its neighbor to send packets to a destination node d, which is multi-hop away, u needs to pay a price to purchase the forwarding service. Such a neighbor is called a *forwarding neighbor* for u. Since a transmitting node knows the minimum power to reach each of its forwarding neighbors from their feedbacks, it uses as low power as possible every time.

Because energy is the overwhelming concern for nodes in a MANET, we define that the price of the network service should represent the amount of power consumed by a service provider. One unit of payment should be able to buy one unit of power. The payment can be authenticated by any seller. To simplify the analysis in this research, we use the power value as a measurement of payments directly. How to transfer and authenticate the payment is out of the scope of this dissertation. We include them into the future work.

We define that for node u, each neighbor v_i has a direction to some fixed angle. The direction can be expressed as $dir_u(v_i)$. There is an angle checker function denoted as $Cone_\alpha(Nei_u)$. It checks whether in the neighbor set N_u there is a gap with degree greater than α between a pair of direction-wise adjacent nodes. If there is such a gap, $Cone_\alpha(N_u)$ returns a TRUE. When a FALSE is returned, there is at least one neighbor in each cone of α around node u.

TRUECON algorithm is shown in Fig. 8. It is the first distributed topology control algorithm to induce selfish nodes in a MANET to reveal their true costs.

Figure 9 gives an example of running TRUECON algorithm on a network node u.

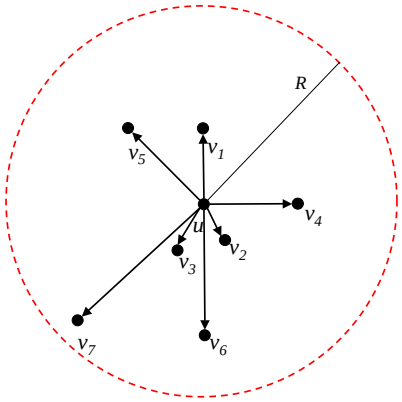
```
TRUECON(α)
 1. N_u = M_u = φ
 2. broadcast Hello with full power
 3. receive Acks and record the neighbors into N_u
 4. if (N_u == φ)
 5.  return
 6. sort N_u by P̂_{u,v_i} in a non-decreasing order, ∀v_i ∈ N_u
 7. while(Cone_α(M_u) AND N_u ≠ φ)
 8.    v_i = DEQUEUE(N_u)
 9.    M_u = M_u ∪ {v_i}
10. if (N_u == φ)
11.  return
12. mark all the nodes in M_u and assign their payment as ∞
13. while(( ∃v_k ∈ M_u, v_k is marked and has no payment decided) AND (N_u ≠ φ))
14.    v_j = DEQUEUE(N_u)
15.    if (( ∃v_l ∈ M_u) AND ( not Cone_α((M_u − {v_l}) ∪ v_j)))
16.         w_{v_l} = P̂_{u,v_j}  // w_{v_l} is the payment of node v_l
17.    M_u = M_u ∪ v_j
18. if (∃v_m ∈ M_u, v_m is marked, w_{v_m} = ∞)
19.     w_{v_m} = P_max
20. P_u = max(P̂_{u,v_k}), ∀v_k ∈ M_u, v_k is marked
```

Fig. 8. TRUECON algorithm running on node u.

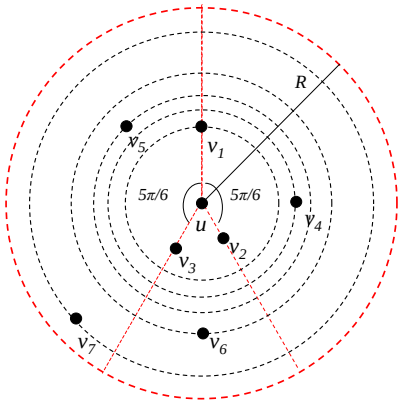
At first, u broadcasts a *Hello* message using its maximum power P_{max}, and announces P_{max} in the *Hello* message. A neighbor node v_i measures the received signal strength P_r and calculate the minimum power P_{u,v_i}, by which u can reach v_i. v_i acknowledges u by sending back an *Ack* message, in which it declares a value $\hat{P}_{u,v_i}$ based on P_{u,v_i}. $\hat{P}_{u,v_i}$ may not equal P_{u,v_i}.

Upon receiving each *Ack*, u saves the replying node information into the set N_u. Due to packet collisions and protocol back-off time, the *Ack*s may arrive in arbitrary order. Without loss of generality, u have $N_u = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}$ before it runs line 6 of TRUECON.

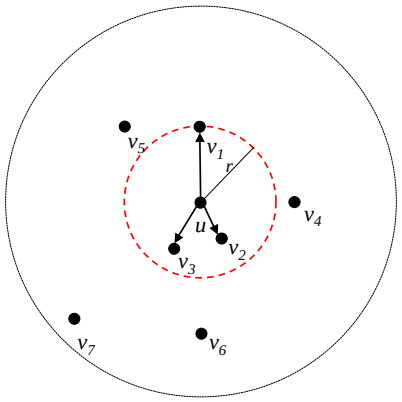
At line 6, u sorts the nodes in N_u by their claimed power value $\hat{P}_{min}$. This value reflects the distance from u to each of its neighbors. Because of the radio attenuation, the farther a neighbor, the greater its value. If each neighbor declares



(a)



(b)



(c)

Fig. 9. Example of running TRUECON algorithm on node u.

its value correctly, then after the sort we have

$$N_u = \{v_2, v_3, v_1, v_4, v_5, v_6, v_7\}$$

We define $\alpha = \frac{5\pi}{6}$ in this example. Li et al. [48] prove that $\frac{5\pi}{6}$ is a tight bound for such topology control algorithms that keep only the nearest neighbors without the knowledge of their geographical locations. We call a $\frac{5\pi}{6}$ cone a *critical cone* and denote the condition of finding at least one neighbor in each critical cone as *direction constraint* or *d. c.*. At line $7-9$, u checks whether there is an angle between a pair of direction-wise adjacent neighbors greater than $\frac{5\pi}{6}$. All the neighbors are checked in the sorted order, which represents the order of distance.

In the Fig. 9 example, when v_1 is added into M_u, $\angle v_1uv_2 = \angle v_1uv_3 = \frac{5\pi}{6}$ and $\angle v_2uv_3 = \frac{\pi}{3}$. Thus, after line 9, M_u contains the closest nodes $\{v_2, v_3, v_1\}$, which make function $Cone_\alpha(M_u)$ return a FALSE. At this point, TRUECON finds the same neighbor set as CBTC finds so that TRUECON inherits the connectivity characteristics of CBTC.

Though we have discovered the nearest neighbor set, which assure the connectivity of a network graph, we need to decide the payment of each node in order to stimulate their collaborations. Line 12 to 17 of TRUECON algorithm implement a VCG mechanism in the context of MANET topology control.

M_u increments by one node every time. Without loss of generality, v_j is the claimed closest neighbor among all the node left in N_u. After adding v_j, if there exist a node v_k in M_u and v_k could be excluded so that $Cone_\alpha(M_u - \{v_k\} \cup v_j)$ is a FALSE, then payoff for v_k is equal to v_j's claimed power value P_{u,v_j}. Since v_k is already in M_u and the algorithm processes nodes in a non-decreasing order, $P_{u,v_k} \leq P_{u,v_j}$.

In the example of Fig. 9., when node v_4 is entered into M_u, it can replace the v_2. Then v_4's claimed power value decides v_2's payment w_{v_2}. In the same way, v_5

determines v_1's payment w_{v_1} and v_6 determines v_3's payoff w_{v_3}. After processing v_6, the algorithm reaches the last line. Node u adjusts its transmission power to be the maximum claimed power value of nodes in M_u. If every node reports correctly, then at the end of TRUECON, u sets its power P_u as P_{u,v_1}.

In TRUECON, after a node's payment is set, it is not changed between two rounds of *Hello* messages. To reduce the radio interference caused by sending *Hello*s, we can lower the transmission power of *Hello* messages to the power TRUECON decides. In a MANET, network nodes can move around. Therefore, between two consecutive rounds of *Hello-Ack* exchange, the nearest neighbor set may change. Then the transmission powers of *Hello* messages and data packets need to change accordingly. We prove that no matter what circumstances, any node in the neighbor set cannot increase its benefit by cheating. We give the formal proof in the next section.

It is observed that in the example of Fig. 9., every neighbor in M_u has a payment decided before the algorithm ends. However in some cases, the algorithm may stop before each critical neighbor finds a substitute and sets its payoff. Then the payment for those neighbors would be equal to the maximum power P_{max}.

Fig. 10. gives another example of u running TRUECON. In this case, u processes its neighbors in an order of $v_1, v_2, v_3, v_4, v_5, v_6$ respectively. As it reaches v_4, the direction constraint is satisfied at the first time. It is observed that v_3 and v_2 are substitute for each other. Due to the farther distance of v_3 to u, $d(v_3, u) > d(v_2, u)$, the declared power value of v_3 is greater than that of v_2, $\hat{P}_{v_3} > \hat{P}_{v_2}$. Then v_2's payment is chosen by TRUECON as $\hat{P}_{v_3}$. Though TRUECON reach v_2, v_3 before v_4, the payment function cannot start because the direction constraint has not been met yet.

After running TRUECON, if node u receives packets from one of its forwarding

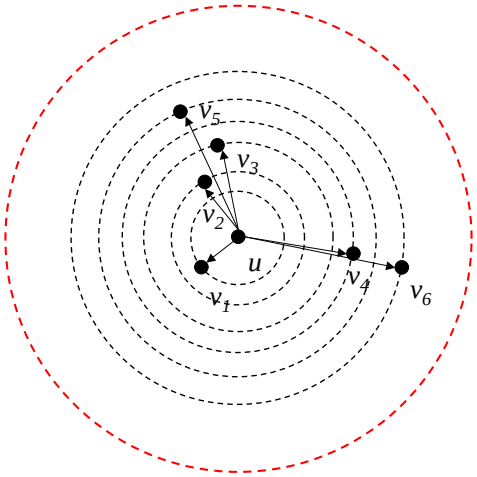


Fig. 10. An example of running TRUECON on node u. The outer dash line circle represents the communication range of u while transmitting at its full power level. An inner dash line circle represents the minimum communication range of u when it needs to talk to the neighbor which resides on the circle.

neighbor, say v_i, u needs to sign on the payment w_{v_i}, which is set beforehand. In TRUECON, we let the source node pay the price along the path. The endorsement of a node on the payment of its predecessor is very important. We discuss this issue in later sections. The monetary transfers are critical to generate cooperative incentives of rational nodes.

2. Analysis of TRUECON Algorithm

a. TRUECON Preserves the Network Connectivity

We denote the network graph, in which each node transmits using its full power P_{max}, as as G_R. After running TRUECON, a network node reduce its transmission power to P', $P' \leq P$. The derived network graph is denoted as G_r then.

Theorem C.1 *If in G_r for each cone not greater than $\frac{5\pi}{6}$ there is a neighbor node, G_r preserves the connectivity of G_R. Node u and v are connected in G_r if and only if*

they are connected in G_R.

Proof The TRUECON works in the same way as CBTC algorithm to discover neighbors. In figure 8, before line 12, TRUECON obtains the same neighbor set for each node as CBTC. The set of nodes is saved in M_u. After that line, M_u never decreases. Therefore, the result graph of TRUECON at least contains the graph derived by CBTC.

Then the network connectivity of TRUECON follows CBTC. Since CBTC preserves the network connectivity, TRUECON preserves the network connectivity too.

b. TRUECON Is Truthful

In addition to a topology control algorithm, TRUECON is a truthful mechanism as well. The selection function of the mechanism chooses an outcome to minimize the nominal transmission power of a network node, as long as the direction constraint is satisfied.

By definition, TRUECON is a direct-revelation mechanism because it lets each participant announce its private type, which is the minimum transmission power in this case. The payment is decided based on the declared values. Without loss of generality, we let node u run TRUECON. The result neighbor set of u is Nei_u, $Nei_u = \{v_1, v_2, \ldots, v_n\}$. The utility function of a neighbor $v_i, (1 \leq i \leq n)$ is $u(v_i)$. Since we assume every network node has an identical radio component, the link is symmetric. If node u can communicate to node v using transmission power $p_{u,v}$, then v can send packets to u with the same power. So $p_{u,v} = p_{v,u}$. In TRUECON, when node v_i receives a *Hello* message from u, it measures the received signal and estimates the minimum power u can use to reach it. The calculated power value is also what it needs to send packets to u. This power is the cost for v_i to forward packets to u and

only v_i knows its value. As we discussed previously, the declared value $\hat{P}_{u,v_i}$ in *Ack* is not necessary to be equal to P_{u,v_i}. Node u needs to decide v_i's payment w_{v_i} based on v_i's and others' announcements. Hence,

$$u(v_i) = -P_{v_i}(o, P_{v_i,u}) + t_{v_i}(\hat{P}) \tag{4.1}$$

In 4.1, the first part is v_i's cost function representing the power it needs to consume. So it should be a non-positive value. And the second part is the payment function of v_i.

We observe $u(v_i)$ is a quasi-linear function. As Parkes states in [29]:

> "The Groves mechanisms are the only allocatively-efficient and strategy-proof mechanisms for agents with quasi-linear preferences and general valuation functions, among all direct-revelation mechanisms. "

The VCG family mechanisms are simply called the Groves mechanisms in [29]. Thus if TRUECON implements a VCG mechanism, we can guarantee the efficiency and truthfulness of TRUECON.

The selection rule of TRUECON is $k : P_{v_1} \times P_{v_2} \times \ldots \times P_{v_n} \rightarrow \mathcal{K}$ and the payment rule is $t_i : P_{v_1} \times P_{v_2} \times \ldots \times P_{v_n} \rightarrow \mathbb{R}$, for each neighbor v_i. Node v_i reports the power value $\hat{P}_{v_i,u}$ with its strategies s_{v_i}, then $\hat{P}_{v_i,u} = s_{v_i}(P_{v_i,u})$. $\hat{P}_{-v_i,u}$ denotes the reported value of all the neighbor nodes except i.

The selection rule of TRUECON computes:

$$k^* = arg \min_{k \in \mathcal{K}} \sum_i P_{v_i}(k, \hat{P}_{v_i,u}), v_i \in Nei_u, with\ a\ direction\ constraint \tag{4.2}$$

The direction constraint demands that there is no gap greater than $\frac{5\pi}{6}$ among the neighbors. k^* is the choice that minimize the total reported power over the minimal satisfactory neighbor set.

The payment rule in TRUECON mechanism is defined as:

$$t_{v_i}(\hat{P}) = h_{v_i}(\hat{P}_{-v_i,u}) - \sum_{j \neq i} P_{v_j}(k^*, \hat{P}_{v_j,u}) \tag{4.3}$$

$h_{v_i}(\hat{P}_{-v_i,u})$ is a function over all the neighbor nodes except v_i. With $h_{v_i}(\hat{P}_{-v_i,u})$, the payment function t_{v_i} picks v_i's first substitute, which has a greater declared power and keeps the direction constraint satisfied without v_i. t_{v_i} guarantees the Individual Rationality (IC) because if a node participates the mechanism and reports correctly, its expected utility is always non-negative. This is a desirable property for mechanisms to stimulate participation. Also it shows that a participant is always overpaid by a payment higher than its cost. However, as we prove later, the overpayment has an upper bound against the total cost.

By substitution, we have

$$\begin{aligned}
u_{v_i}(\hat{P}_{v_i}) &= -P_{v_i}(k^*(\hat{P}), P_{v_i,u}) + t_{v_i}(\hat{P}) && (4.4)\\
&= -P_{v_i}(k^*(\hat{P}), P_{v_i,u}) + (h_{v_i}(\hat{P}_{-v_i,u}) - \sum_{j \neq i} P_{v_j}(k^*(\hat{P}), \hat{P}_{v_j,u})) && (4.5)\\
&= \begin{cases} -P_{v_i,u} - \sum_{j \neq i} P_{v_j}(k^*(\hat{P}), \hat{P}_{v_j,u}) + h_{v_i}(\hat{P}_{-v_i,u}) & \text{if } v_i \text{ is selected} \\ 0 & \text{otherwise} \end{cases} && (4.6)
\end{aligned}$$

The first two terms are the negative part of the utility function because the power value represents the cost of each node while serving others. We can ignore the h_i function, as it has nothing to do with v_i. If v_i wants to maximize its utility, it must minimize the absolute value of the negative part. Hence, v_i want to find a strategy to solve:

$$\min_{s_{v_i} \in S_{v_i}} \left[P_{v_i}(k^*(\hat{P}_{v_i,u}, \hat{P}_{-v_i,u}), P_{v_i,u}) + \sum_{j \neq i} P_{v_j}(k^*(\hat{P}_{v_i,u}, \hat{P}_{-v_i,u}), \hat{P}_{v_j,u}) \right] \quad (4.7)$$

$$= \min_{s_{v_i} \in S_{v_i}} \left[P_{v_i}(k, P_{v_i,u}) + \sum_{j \neq i} P_{v_j}(k, \hat{P}_{v_j,u}) \right] \quad (4.8)$$

If 4.7 is solved by a single strategy $\bar{s}_{v_i}$, v_i can secure its maximum expected utility no matter what strategies other nodes play.

v_i can affect the mechanism outcome, $k^*(\hat{P}_{v_i,u}, \hat{P}_{-v_i,u})$, by reporting $P_{v_i,u}$ as different values. However, only when $\hat{P}_{v_i} = P_{v_i}$, the mechanism explicitly solve:

$$\min_{k \in K} \sum_i (\hat{P}) \quad (4.9)$$

$$= \min_{k \in K} \left[P_{v_i}(k, \hat{P}_{v_i,u}) + \sum_{j \neq i} P_{v_j}(k, \hat{P}_{v_j,u}) \right], \textit{with d. c.} \quad (4.10)$$

Since the neighbor's direction is detected by the node running TRUECON, the neighbors' strategies have no influence on the direction constraint. As a result, Truth-revelation is the *dominant strategy* of v_i, whatever the reported $\hat{P}_{-v_i,u}$. Then we prove the following theorem.

Theorem C.2 *TRUECON mechanism is strategy-proof.*

In TRUECON, no node can obtain a higher expected utility by cheating as long as there is another node to be able to replace it. Please note that we assume there is no collusion among all network nodes. Everyone is on its own when deciding what strategy to play.

Using the example in Fig. 9., we demonstrate how TRUECON achieve truthfulness. Let d denotes the distance between nodes. Then, $d(u, v_2) < d(u, v_3) <$

$d(u, v_1) < d(u, v_4), < d(u, v_5) < d(u, v_6) < d(u, v_7)$. When all the node report correctly, we have $\hat{P}_{v_2,u} < \hat{P}_{v_3,u} < \hat{P}_{v_1,u} < \hat{P}_{v_4,u} < \hat{P}_{v_5,u} < \hat{P}_{v_6,u} < \hat{P}_{v_7,u}$. By the design of TRUECON, the minimal set of nodes, which satisfy the direction constraint, includes v_1, v_2, v_3. The participation of v_4 can spare v_2 without violation of the direction constrain. Then the payment of v_2 equals to v_4's reported value, $\hat{P}_{v_4,u}$.

If v_2 intentionally reports a value smaller than the true value, $\hat{P}_{v_2,u} < P_{v_2,u}$ and v_4 tells the truth, v_2's payment is not changed because of $\hat{P}_{v_2,u} < P_{v_2,u} < \hat{P}_{v_4,u}$. The directions of v_2 and v_4 are measured by u. u always knows that v_4 is a substitute for v_2.

If v_2 reports a greater value, $\hat{P}_{v_2,u} > P_{v_2,u}$ and v_4 tells the truth, we need to check two cases. First, $\hat{P}_{v_2,u} < \hat{P}_{v_4,u}$. Then the payment for v_2 is still set as $\hat{P}_{v_4,u}$. Second, if v_2 overstates too much and makes $\hat{P}_{v_2,u} > \hat{P}_{v_4,u}$. Then TRUECON selects v_4 together with v_1, v_3 and assigns v_4's payment as $\hat{P}_{v_2,u}$. Since when TRUECON terminates, v_2 has no assigned payment, u is not going to endorse v_2 for anything. That causes v_2 not to be paid. The nominated neighbor set v_3, v_1, v_4 satisfies the direction constraint. Then by Theorem C.1, it preserves the network connectivity for u. Consequently, v_2 excludes itself from the forwarding neighbors and loses the payment it could earn.

While v_4 is cheating, the truth-revelation is still the best strategy for v_2. If v_4 reports a $\hat{P}_{v_4,u}$, which is greater than $P_{v_4,u}$, and v_2 reports correctly, the payment of v_2 is still equal to the announced power value of v_4.

When v_4 understates by revealing a $\hat{P}_{v_2,u}$, $\hat{P}_{v_2,u} < \hat{P}_{v_4,u} < P_{v_4,u}$, and v_2 reports correctly, v_2 is still selected and secures a payment, which is greater than its cost. v_4 may want to be chosen by u desperately and declares a very small $\hat{P}_{v_4,u}$, $\hat{P}_{v_4,u} < P_{v_2,u} = \hat{P}_{v_2,u} < P_{v_4,u}$. Then u selects v_4 as a forwarding neighbor and pays it $\hat{P}_{v_2}$. The utility of v_2 is zero, while that of v_4 is a negative value, $-P_{v_4} + P_{v_2}$. In other words, v_4 is punished by being underpaid. This is unacceptable for a rational node.

Though v_2 is not selected, it does not lose anything by keeping its utility as zero. If v_2 makes a counterattack by reporting a smaller $\hat{P}_{v_2,u}$, $\hat{P}_{v_2,u} < \hat{P}_{v_4,u}$, its payment cannot compensate its cost.

Apparently, as v_2 is rational, the only strategy it follows is to report correctly all the time. The same strategy also applies to other nodes selected by TRUECON. No matter how they report, they cannot make a better expected utility.

TRUECON also has its limit. In some case a node may obtain the ultimate claim power because of its physical location.

Lemma C.3 *In a graph G_R, if a node has only one neighbor within a cone of $\frac{5}{6}\pi$, the truthfulness cannot be achieved while preserving the network connectivity.*

Proof We assume a truthful mechanism $\mathcal{M}$ is available to assure both connectivity and truthfulness in such a graph. Then truth-revelation is a dominant strategy for v.

Since $\frac{5}{6}\pi$ is a tight bound for preserving network connectivity, the single neighbors in a cone of $\frac{5\pi}{6}$ is critical. In other words, if one of such kind of neighbors refuses to forward packets, then the network may partitions. Therefore, the neighbor may claim an arbitrarily high payment in favor of its own utility. As a result, the truthfulness is broken. This contradicts our assumption.

Obviously, TRUECON achieves limited truthfulness. It cannot assure that those critical neighbors are always induced to cooperate by paying them the maximum power value P. Both sides of a trade know that P_{max} is a price, which is high enough to pay off any neighbor's cost. But a critical neighbor may not be satisfied in that it is too important to lose. On the other hand, the node choosing neighbors may delay its payment decision in hope of a new neighbor arriving in the future. Or it may need to pay a higher price than the maximum power if it is affordable for it. Otherwise, it just cuts off the critical neighbor and let the network suffer from a partition.

Lemma C.3 also proves that all the topology control algorithms, which connect to only closest neighbors have such a limit.

c. Scalability of TRUECON

TRUECON is scalable and adaptive. Though the algorithm in Fig. 8. demands a node to transmit a *Hello* message using full power initially, TRUECON can dynamically change the power according to the node density of a network. Intuitively, the sending power of *Hello* messages can be confined at the range to the farthest of the replacement nodes, which decide the payment of the forwarding neighbors. So a node can keep enough neighbors to acknowledge its *Hello* messages and avoid unnecessary packet collisions.

As we expect network nodes are distributed into the coverage area evenly, the node degree can be denoted as a constant D. To find replacements for D neighbors, the *Ack*s number equals constant times of degree D. Then with the growth of the node number n, the number of signaling messages is still $O(1)$.

3. Routing with TRUECON

Each node runs TRUECON locally and adjusts its transmission power to induce a subgraph, which inherits the connectivity of the original network graph. Except for the Hello-Ack exchange and dynamic power adjustment, TRUECON does not have any extra technical requirement so that it is easy to integrate TRUECON with most of the existing MANET routing protocols, such as AODV [43], DSR [26]. In this section, we discuss the design of DSR-TRUECON, a DSR routing protocol with TRUECON enhancement.

a. DSR-TRUECON — the DSR Enhanced with TRUECON

Dynamic Source Routing (DSR) protocol is a reactive routing protocol. In DSR, each network node has a unique ID. When a source node S wants to communicate to a destination node D, which is usually multi-hop away from S, it first looks up its routing table to check whether there is a route from S to D. If there is no such a route, S initiates a route discovery process by broadcasting a Route Request packet (RREQ) into its neighborhood. S adds its ID into an address list in the request packet. The RREQ packet also has a unique request identifier so that each receiver can identify it. Upon receiving a RREQ, a network node checks whether it is the destination. If it is not and does not know a path to D, it inserts its ID into the address list and broadcasts it again. While the RREQ finally reaches the destination D, D replies with a Route Reply packet (RREP) containing all the accumulated route information about the intermediate nodes through which the RREQ passes. The RREP is sent back to S by reversing the path. After S receives a RREP from D a route between them is established. Data packets will be transferred along this discovered path.

TRUECON requires some adaptations of DSR in order to discover a cost efficient route while keeping the incentive-compatible property. TRUECON needs to periodically broadcast, in one hop, the *Hello* messages and collect Acknowledges from the neighborhood. This scheme is supported by most MANET routing protocols. Each TRUECON-enabled node adjusts its transmission power based on the topology in its vicinity.

In a MANET, TRUECON requires some payment transfer facility, which guarantees to deliver the payment to a service provider securely at right amount. By such a facility, the payment can only be taken by the designated node. Other nodes can neither steal nor tamper the payment by all means. We assume there is such an

```
DSR-TRUECON()
  1.   while (true)
  2.    if (received a Route Request message)
  3.      if (this is the destination)
  4.        sum up the total cost and save the RREQ into a table
  5.        reset time T_r
  6.      else if (a RREQ with the same Identification received previously)
  7.        sum up the total cost
  8.        if (the new RREQ has a lower cost)
  9.          set the cost for the last node and append my ID
 10.          broadcast the RREQ
 11.        else
 12.          disregard this message
 13.    else if (receive a Route Reply message)
 14.      set the payment of the predecessor in the RREP and sign on it
 15.      send the RREP to the predecessor
 16.    else if (timer T_r is expired)
 17.      generate a Route Reply message
 18.      copy the route with the smallest cost into the RREP
 19.      set the payment of the predecessor and sign on it
 20.      send the RREP to the predecessor
```

Fig. 11. DSR-TRUECON algorithm for processing Route Request and Route Reply

infrastructure deployed in our system.

In DSR-TRUECON, the source node needs to pay the bill of sending packet along the entire route. Since the source node needs the forwarding service to fulfill its own functions, it is reasonable to charge it as the service consumer.

Fig. 11 presents the DSR-TRUECON algorithm of processing Route Request and Route Reply packets. It is shown that DSR-TRUECON implements a distributed Bellman-Ford algorithm [49] to find a shortest path for a single source in a weighted graph. We use a two-pass scheme to discover the power-efficient path and transfer the payment information.

During the route discovery process, when an intermediate node v receives a RREQ from u, it needs to check the identifier of the packet to determine whether this RREQ has been seen before. If it is a new packet, v records the cost of its predecessor u into the received RREQ packet and appends its own ID. The cost is the power consumption of transmitting packets from u to v. Node v knows u's cost because u

declares this value as $\hat{P}_{u,v}$ when v runs TRUECON beforehand. By Theorem C.2, u must declare correctly. Then a successor always knows the predecessor's cost of the packet transmission. v saves the updated request into a table and broadcasts it into the network.

If v finds that a same identifier has been received previously, it compares the total cost in the newly arrived RREQ with the old ones. If the new RREQ has a lower cost, it travels on a more power-efficient path to reach node v. After updating corresponding fields, v needs to send out this RREQ by broadcasting it again. Otherwise, it just disregards the request.

When the destination node D receives a RREQ, D saves it and sets a timer T_r. The timer is used because D needs to pick the most power-efficient path. The messages traveling on different paths have different delay to get on the destination. Every time a new RREQ with the same identifier arrives, D resets the timer T_r. Finally, when the timer expires, D picks the route with the lowest cost. It records the route in a RREP packet and set the payment of its predecessor. The payment information needs to be signed using the private key of the writing node. This is to prevent the predecessor from manipulating the information to claim more benefit.

The RREP is transmitted to the source node along a reverse path using unicast. Inside the RREP packet, the intermediate nodes on the route set the payment for their predecessors one by one. The node next to the source does not need to do this because the source node is the buyer of the forwarding service. After the RREP arrives at the source node, the IDs of the intermediate nodes are recorded as well as their prices. We assume there is no collusion between any selfish nodes and all the nodes are rational. Then each successor reports the payment of its predecessor correctly because a biased value cannot bring back any extra benefit to it.

By the design of DSR-TRUECON, the routing protocol always finds a most cost-

Table III. THE ROUTE REQUEST OPTION FORMAT FOR DSR-TRUECON

Option Type	Opt Data Len	Identification
Target Address [1]		
Cost[0]		
Address[1]		
Cost[1]		
Address[2]		
Cost[2]		
Address[3]		
...		
Cost[n-1]		
Address[n]		

Table IV. THE ROUTE REPLY OPTION FORMAT FOR DSR-TRUECON

	Option Type	Opt Data Len	L	Reserved
Address[1]				
Payment[1]				
Address[2]				
Payment[2]				
Address[3]				
...				
Payment[n-1]				
Address[n]				
Payment[n]				

efficient (also power-efficient) path in the network. Each node broadcasts a RREQ at least once. In the worst case, a node needs to transmit a RREQ for every other node if an incoming RREQ always reveals a more cost-efficient path than the previous RREQs. Therefore, the message complexity of DSR-TRUE is $O(n^2)$, where n is the number of network nodes.

To accommodate the cost/payment information, the structures of the Route Request and Route Reply messages need to be expanded. The formats of RREQ and RREP packets are shown in Table III and Table IV respectively.

b. Case Study of Routing with DSR-TRUECON

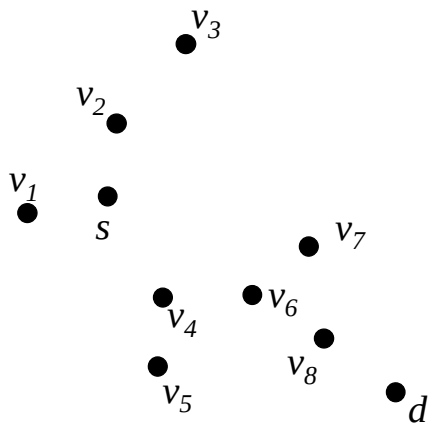


Fig. 12. A MANET with 10 nodes. S is the source node, which have packets to send to the destination node D.

Fig. 12 gives an example of a MANET, in which there are 10 network nodes. Node S has data packets to send to node D, but it does not know a route to D. Fig. 13 shows how the DSR protocol discovers a route from S to D in the example MANET.

S initiates a route discovery by broadcasting a Route Request (RREQ) into the network with its maximum power. Within the communication range of S are

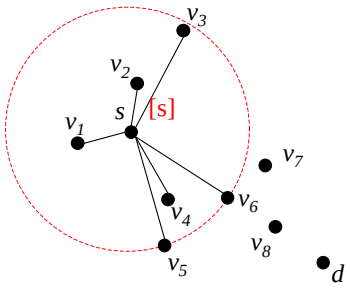
node v_1, v_2, v_3, v_4, v_5 and v_6. They receives the RREQ from S and check whether they are the destination. Since their routing tables are empty at the beginning, they add a record for S into the tables. Then they append their IDs to the RREQ and propagate it by transmitting it as a local broadcast packet. In the six copies of the Route Request, the route information is $[s, v_1], [s, v_2,], [s, v_3], [s, v_4], [s, v_5]$ and $[s, v_6]$ respectively.

Node v_7, v_8 and d are out of the transmission range of S so that they cannot receive the RREQ directly from S. During the second round broadcast, the RREQ reaches these three nodes. Node v_7 and v_8 repeats the same procedures as $v_1 \ldots v_6$. Node D checks the request message and finds it is the intended destination. D generates a Route Reply (RREP) and copy the list of intermediate nodes, without loss of generality, $\{v_6\}$. The RREP is returned to S by traversing the reverse path, $\{d, v_6, s\}$. During the meantime, v_7 and v_8 broadcast separately their copies of the Route Request, including two different routes $[s, v_6, v_7]$ and $[s, v_6, v_8]$.

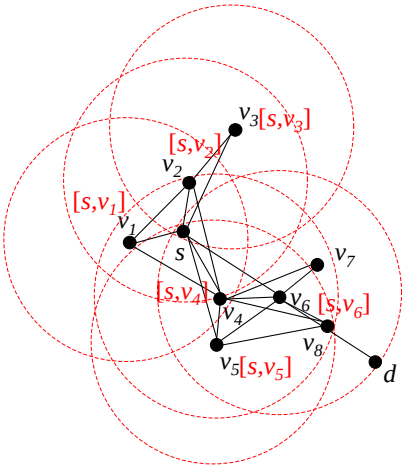
Fig. 14 illustrates the route discover using DSR-TRUECON. DSR-TRUECON has the same routing procedures as DSR. However the transmission range of each node is dramatically reduced as a result of TRUECON. It is observed that the route in Fig. 14.d has more hops than that in Fig. 13, $\{s, v_4, v_6, v_8, d\}$ versus $\{s, v_6, d\}$. This is desirable for saving energy because the transmission power decreases to the αth power of the distance between a transmitter and a receiver, $\alpha \in [2, 6]$.

Comparing Fig. 13.*b* with Fig. 14.*b*, DSR-TRUECON constrains the interference area within a much smaller region than the standard DSR. Alleviation on radio interference can improve the network throughput and shorten the packet delay.

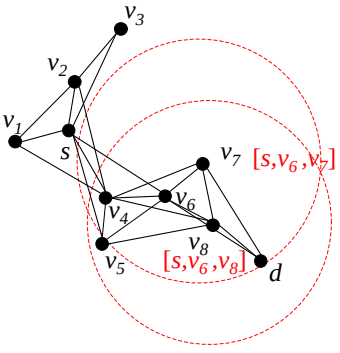
If a node receives two RREQs respectively, it can determine whether they are the same request by checking their identifiers. The request identifier is set by the source node and not changed by intermediate nodes. A Route Request received before may



(a)

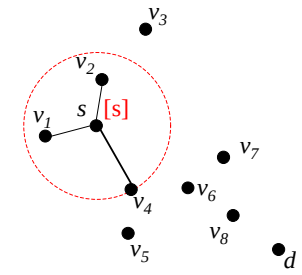


(b)

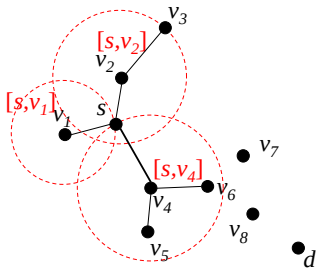


(c)

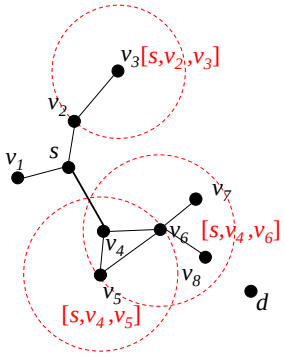
Fig. 13. Routing using DSR for the MANET in Fig. 12.



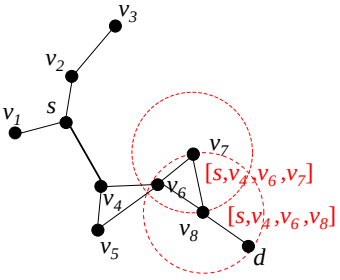
(a)



(b)



(c)



(d)

Fig. 14. Routing using DSR-TRUECON for the MANET in Fig. 12.

be sent out again in DSR-TRUECON if it has a lower cost than others.

c. Overpayment of DSR-TRUECON

DSR-TRUECON guarantees to discover a minimum transmission power (MTP) path. The source node needs to pay whatever price the path turns out in order to assure the Individual Rationality (IR). Obviously, the price of a MTP path is higher than the total cost and not necessary to be the cheapest among all the paths connecting the same source and destination.

Definition C.1 Overpayment *(OP) is the ratio of the total payment against the total cost along a path.*

Then

$$OP_{S,D} = \frac{\sum_{i=1}^{l-1} w_{v_i}}{\sum_{i=0}^{l-1} P_{v_i}} \tag{4.11}$$

In 4.11, w_{v_i} is the payment to node v_i and P_{v_i} is the transmission power of node v_i, $(v_0 = S)$. On a l-hop path, there are $l-1$ nodes transmitting data packets, including the source S and there are $l-2$ nodes earning payment.

The overpayment of DSR-TRUECON could be very high when a forwarding node is paid at the maximum rate and very close to its successor. Fig. 15 shows such a case. Node b, d, e are the forwarding neighbors for a. On the path $\{c, b, a\}$, b is close to its successor a. Though c is near b, it does not satisfy the direction constraint when it takes over b. Therefore, the payment to b is equal to the power to reach a farther replacement node b'. As a result, the overpayment of this path is high.

Network nodes may not be happy if they pay too much for a MTP path and become financially broke fast. In order to bound the overpayment, we revise the TRUECON algorithm to pay a forwarding neighbor by whatever is smaller between the pre-decided payment and the cost to reach its predecessor from its successor along

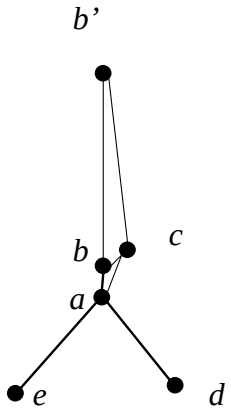


Fig. 15. $\{c, b, a\}$ is of a minimum transmission power path from node c to node a. b', b and a on the same straight line. The angles formed by b, a, d and b, a, e are the same as $\frac{5\pi}{6}$. The distance from b to a is ϵ. In TRUECON, the payment to b is equal to the power on (a, b').

a path. We call the revised algorithm TRUECON-ECO, since it assures the economy of an outcome. Then we prove that the overpayment can be bounded for the source node.

Lemma C.4 *TRUECON-ECO is strategy-proof.*

Proof As TRUECON, a node u periodically sends *Hello* messages into its neighborhood and collects *Ack*s. A neighbor v_i announces the transmission power $\hat{P}_{v_i,u}$ in the *Ack*. The selection function, $k : \hat{P}_{v_1} \times \hat{P}_{v_2} \ldots \hat{P}_{v_n} \rightarrow \mathcal{K}$, chooses the smallest set of forwarding neighbors, which make the direction constraint satisfied. Let k^* be the outcome of TRUECON-ECO mechanism, and

$$k^* = arg \min_{k \in \mathcal{K}} \sum_i \hat{P}_{v_i}(k, \hat{P}_{v_i,u}),\ v_i \in Nei_u,\ with\ d.\ c. \tag{4.12}$$

The payment function t_{v_i} of TRUECON has two choices. It can assigns the payment to the forwarding neighbor v_i as the announced power value of the first

node v_j, which can replace v_i without violation of the direction constraint. Then decided price of v_i is $w_{v_i}(k^*, P_{v_i,u}) = \hat{P}_{v_j,u}$. Or t_{v_i} waits until a path going through v_i and u, where the t_{v_i} is running. The payment will not be delivered until a node is selected on a path and starts forwarding data packets.

Suppose v_i is on a path, the predecessor of v_i is v_h, $v_h \neq v_j$, and the successor of v_i is u. Node u can communicate to v_h using its maximum power. So u has received v_j's announce power $\hat{P}_{v_j,u}$ in the past. Since u is the node behind v_i on the path and needs to endorse v_i's payment, it compares $\hat{P}_{v_j}$ with $\hat{P}_{v_h}$ and decides on the smaller value between them.

The utility of a node i equals the sum of its payment and its cost. Then

$$u_{v_i}(k^*, P_{v_i}) = P_{v_i,u} + t_i(k^*, \hat{P}_{v_i,u})$$

Apparently, TRUECON-ECO is a direct-revelation mechanism, in which every node has a quasi-linear utility function. The outcome function of TRUECON-ECO is in the same form as TRUECON. The payment function assigns the payment to a selected node based on the other nodes' declared values.

The only difference between TRUECON and TRUECON-ECO is the payment function t_{v_i}. By 4.3, a payment function of a VCG mechanism consists of two parts. One is an arbitrary function on all the reported values, except $\hat{P}_{v_i}$. The revision of TRUECON-ECO comparing with TRUECON is right on the $h(.)$ function. Consequently, it offsets the difference and keeps TRUECON-ECO as a VCG mechanism.

TRUECON-ECO belongs to the VCG mechanism family, which is *strategy-proof* for direct-revelation mechanisms with quasi-linear utility functions. So TRUECON-ECO is *strategy-proof.*

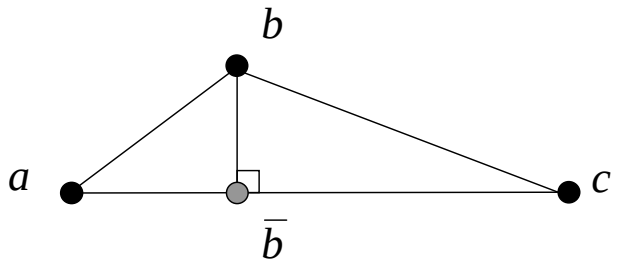


Fig. 16. $\{c, b, a\}$ is of a part of a minimum transmission power path from node S to node D.

We denote the DSR routing protocol with TRUECON-ECO integration as DSR-TRUECON-ECO.

Theorem C.5 *In DSR-TRUECON-ECO, the upper bound of the overpayment along a MTP path is* 2^{α}.

We prove that the overpayment for DSR-TRUECON-ECO has an upper bound, which varies on different radio propagation models.

For the scenario in Fig. 16, we let $\bar{b}$ be the projection of b on segment (a, b). The source node a is two-hop away from the destination node c. The payment to the forwarding node b is the same as the transmission power on edge (a, c). The cost of this route equals to the sum of the transmission power on (a, b) and (b, c). By (2.11), we have

$$\begin{aligned} OP_{a,c} &< \frac{d_{a,c}^{\alpha}}{d_{a,\bar{b}}^{\alpha} + d_{\bar{b},c}^{\alpha}} && (4.13) \\ &\leq \frac{d_{a,c}^{\alpha}}{(\frac{1}{2}d_{a,c})^{\alpha} + (\frac{1}{2}d_{a,c})^{\alpha}} && (4.14) \\ &= 2^{\alpha-1} && (4.15) \end{aligned}$$

Since $\alpha \in [2, 6]$, $OP_{a,c}$ varies between 2 and 32.

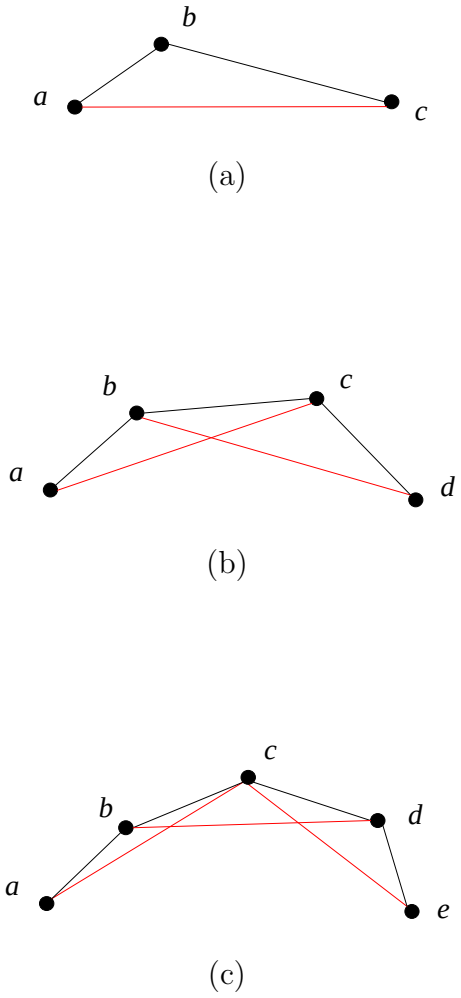


Fig. 17. Case study of the overpayment during routing. The lines connecting (a, b), (b, c), (c, d), and (d, e) represent the minimum energy path from node a to the last node while the lines connecting (a, c), (b, d) and (c, e) represent the Euclidean distance on which the payment value is based.

Fig. 17 shows more scenarios in MANETs. In Fig. 17.a, the overpayment OP for route $\{a, b, c\}$ is

$$OP_{a,c} = \frac{(d_{a,c})^\alpha}{(d_{a,b})^\alpha + (d_{b,c})^\alpha} \tag{4.16}$$

As a, b, c form a triangle, we have

$$d_{a,c} < d_{a,b} + d_{b,c} \tag{4.17}$$

In Fig. 17.b the route between the source node a and the destination d has three hops. We have

$$OP_{a,d} = \frac{(d_{a,c})^\alpha + (d_{b,d})^\alpha}{(d_{a,b})^\alpha + (d_{b,c})^\alpha + (d_{c,d})^\alpha} \tag{4.18}$$

Similarly, in In Fig. 17.c,

$$OP_{a,e} = \frac{(d_{a,c})^\alpha + (d_{b,d})^\alpha + (d_{c,e})^\alpha}{(d_{a,b})^\alpha + (d_{b,c})^\alpha + (d_{c,d})^\alpha + (d_{d,e})^\alpha} \tag{4.19}$$

While we use the free-space radio propagation model, in formulas α is equal to 2. By 4.17, for the scenario in Fig. 17.a, we have

$$d_{a,c}^2 < (d_{a,b} + d_{b,c})^2 \tag{4.20}$$

Thus,

$$\frac{d_{a,c}^2}{d_{a,b}^2 + d_{b,c}^2} < 1 + \frac{2d_{a,b}d_{b,c}}{d_{a,b}^2 + d_{b,c}^2} \tag{4.21}$$

As $d_{a,b}^2 + d_{b,c}^2 \geq 2d_{a,b}d_{b,c}$, then

$$OP_{a,c} \leq 2 \tag{4.22}$$

This result conforms to (4.15). If the source node a is connected to c when they transmit using the maximum power and there is only one forwarding node between them after TRUECON terminates, the overpayment on such a route cannot be greater than two times of the cost of a minimum power path.

By substitution, we have

$$\begin{aligned} OP_{a,d} &< \frac{2d_{a,b}^2 + 2d_{b,c}^2 + 2d_{b,c}^2 + 2d_{c,d}^2}{d_{a,b}^2 + d_{b,c}^2 + d_{c,d}^2} && (4.23) \\ &= 2 + \frac{2d_{b,c}^2}{d_{a,b}^2 + d_{b,c}^2 + d_{c,d}^2} && (4.24) \\ &< 4 && (4.25) \end{aligned}$$

Similarly, we have

$$\begin{aligned} OP_{a,e} &< 2 + \frac{2d_{b,c}^2 + 2d_{c,d}^2}{d_{a,b}^2 + d_{b,c}^2 + d_{c,d}^2 + d_{d,e}^2} && (4.26) \\ &< 4 && (4.27) \end{aligned}$$

We apply the result to the general graph. The path length is denoted as L.

$$OP \leq \begin{cases} 2 & L = 2 \\ 4 & L > 2 \end{cases} \quad (4.28)$$

When the radio propagation model is a two-way reflection model, due to the radio attenuation, transmission power varies as the fourth power of the distance.

By 4.17, for the scenario in Fig. 17.a we have

$$d_{a,c}^4 < (d_{a,b} + d_{b,c})^4 \quad (4.29)$$

$$= d_{a,b}^4 + d_{b,c}^4 + 4d_{a,b}^3 d_{b,c} + 6d_{a,b}^2 d_{b,c}^2 + 4d_{a,b} d_{b,c}^3 \quad (4.30)$$

Then,

$$\begin{aligned}
OP_{a,c} &= \frac{d_{a,c}^4}{d_{a,b}^4 + d_{b,c}^4} && (4.31)\\
&< \frac{d_{a,b}^4 + d_{b,c}^4 + 4d_{a,b}^3 d_{b,c} + 6d_{a,b}^2 d_{b,c}^2 + 4d_{a,b} d_{b,c}^3}{d_{a,b}^4 + d_{b,c}^4} && (4.32)\\
&= 1 + \frac{2d_{a,b} d_{b,c}(2d_{a,b}^2 + 2d_{b,c}^2 + 3d_{a,b} d_{b,c})}{d_{a,b}^4 + d_{b,c}^4} && (4.33)\\
&\leq 1 + \frac{2d_{a,b} d_{b,c}(2d_{a,b}^2 + 2d_{b,c}^2 + \frac{3}{2}d_{a,b}^2 + \frac{3}{2}d_{b,c}^2)}{d_{a,b}^4 + d_{b,c}^4} && (4.34)\\
&= 1 + \frac{7d_{a,b} d_{b,c}(d_{a,b}^2 + d_{b,c}^2)}{d_{a,b}^4 + d_{b,c}^4} && (4.35)\\
&\leq 1 + \frac{\frac{7}{2}(d_{a,b}^2 + d_{b,c}^2)(d_{a,b}^2 + d_{b,c}^2)}{d_{a,b}^4 + d_{b,c}^4} && (4.36)\\
&= 1 + \frac{7}{2} + \frac{2d_{a,b}^2 d_{b,c}^2}{d_{a,b}^4 + d_{b,c}^4} && (4.37)\\
&\leq \frac{11}{2} && (4.38)
\end{aligned}$$

By substitution, for the scenarios in Fig. 17.b and Fig. 17.c, we have

$$\begin{aligned}
OP_{a,d} &< \frac{\frac{11}{2}d_{a,b}^4 + \frac{11}{2}d_{b,c}^4 + \frac{11}{2}d_{b,c}^4 + \frac{11}{2}d_{c,d}^4}{d_{a,b}^4 + d_{b,c}^4 + d_{c,d}^4} && (4.39)\\
&= \frac{11}{2} + \frac{\frac{11}{2}d_{b,c}^4}{d_{a,b}^4 + d_{b,c}^4 + d_{c,d}^4} && (4.40)\\
&< 11 && (4.41)
\end{aligned}$$

And,

$$\begin{aligned}
OP_{a,e} &< \frac{11}{2} + \frac{\frac{11}{2}d_{b,c}^4 + \frac{11}{2}d_{c,d}^4}{d_{a,b}^4 + d_{b,c}^4 + d_{c,d}^4 + d_{d,e}^4} && (4.42)\\
&< 11 && (4.43)
\end{aligned}$$

By 4.31 - 4.43, the total payment of a MTP path cannot exceed 11 times of the total cost along the path, while the two-ray reflection radio propagation model applies. As a result, we have

$$OP \leq \begin{cases} \frac{11}{2} & L = 2 \\ 11 & L > 2 \end{cases} \tag{4.44}$$

The overpayment has a significant impact on the usability of a mechanism. If a mechanism cannot restrain its overpayment, a node may run of money quickly and cannot afford any form of communication. Then the performance of the whole network degrades. In TRUECON-ECO, even though a source node does not know how much the total cost of a path is, it knows it cannot pay more than 2^{α} times of the total cost. An bound of the overpayment is also important for deciding how much start funding needs to be deposited for every node in a network.

D. Simulation of TRUECON

We simulate DSR-TRUECON-ECO in MANETs to evaluate the system performance from the perspectives of topology control and routing. As a reference, we also simulate MANETs, in which every node transmits using the maximum power.

In our experiments, network nodes are distributed uniformly, except a source node and a destination node, into a $600m \times 600m$ area. Each node has an identical radio component, which has a transmission range of $150m$. All the nodes are stationary and do not move throughout the experiments.

A node can adjust its transmission power continuously. Though in real world a wireless device may not be able to alter its emission power gradually, changing the sending power at different levels is feasible. To simplify the analysis, we grant every

node a total control over their power.

A node can measure the received signal strength and the direction, from which a packet comes. It reduces the communication power based on locally information. After every node has decided its power level, we measure the induced network graph and compare it with the original graph.

After TRUECON terminates at each node, a source node starts a route discovery to find a path to a destination node. This pair of nodes is intentionally placed on different sides of a network such that a path between them always has multiple hops. By the design of DSR-TRUECON-ECO, the path is a MTP path. The total cost, sum of transmission power, along the path is compared with that in the original graph, in which each node communicates using the maximum power.

We investigate the result data several metrics, which are average communication range, average node degree, overpayment on a path from S to D, hop ratio and cost ratio. The total number of network nodes varies from 50 to 300. The figures on pages 69-75 present the simulation results. Each point on the graphs represents an average value of 100 runs.

Fig. 18 shows the average communication range of each node at different node densities. As the node density rises, the communication range decreases. In the sparse network graphs, the average Euclidean distance between different nodes is farther than that in the dense graph. So in sparse network, a node is expected to have a smaller neighbor set at the maximum transmission power and need to keep a longer communication range in order to maintain the connectivity. While there are many nodes in network, each node holds a larger neighbor set at the maximum transmission power. It can drop off many nodes without degrading the network connectivity.

Fig. 19 shows the normalized transmission power with different radio propagation models. In the free space model, the path loss exponent α equals 2. In the simulation,

the shortest average communication range is about 41 meters when the number of network nodes is 300. It is below one third of the maximum range. It allows a node to save about 90 percent of its transmission power without the concern of being separated from the rest part of a network. When come to the two-ray ground reflection model the difference is even more significant because α is equal to 4. Though in a real world scenario, the minimum transmission power may not be achieved due to the irregularity of radio propagation, a shorter range does means much less power. Therefore shortening the communication range is still an attractive means to save energy.

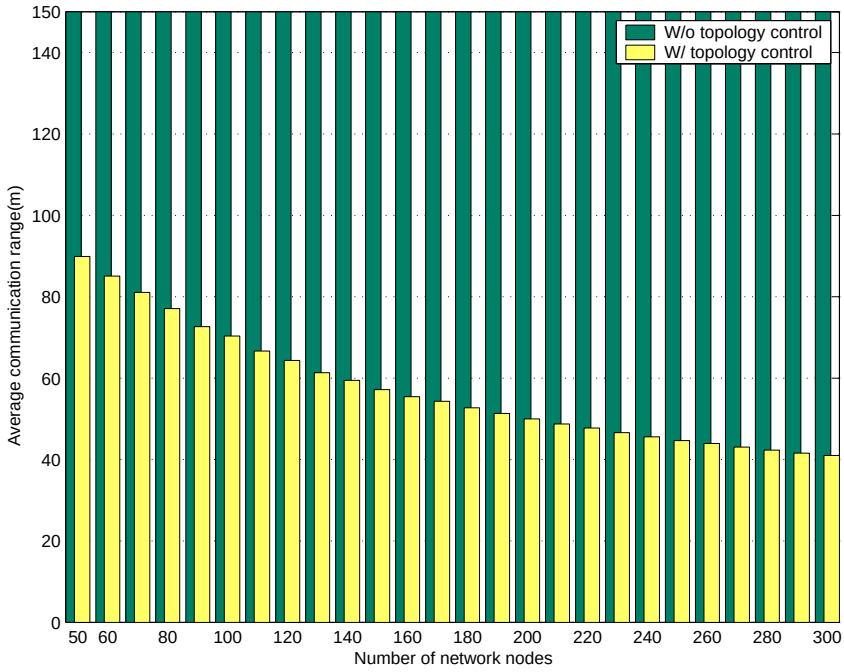


Fig. 18. Average communication range.

Fig. 20 plots the average degree at different node density. Without the topology control mechanism, the node degree increases linearly as the node density increases. The higher connection degree the higher probability of packet collisions and the longer packet delay. The network throughput deteriorates dramatically at a high degree.

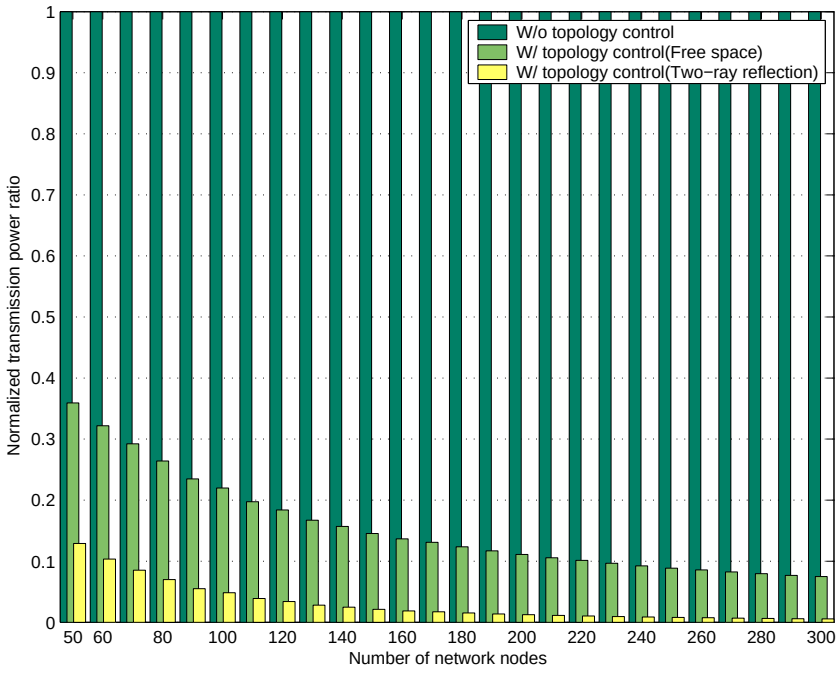


Fig. 19. Average power ratio.

Using TRUECON topology control mechanism, the node degree almost stays as a constant value.

Figs. 21 - 23 show the simulation results in term of the overpayment. The bars with two different colors in Fig. 21 show the average values of the overpayment along a path using the free space model and the two-ray ground reflection model respectively. Fig. 22 and Fig. 23 display the average values along with standard deviations. As we have proved, with the free space model, the overpayment cannot be greater than 4. For the two-ray ground reflection model the upper bound is 11. Experiment results conform to those bounds.

Fig. 24 demonstrates the normalized hops of a TRUECON MTP path against the MTP path before using TRUECON. They are for the same pair of source and destination in the same network. Fig. 25 shows the cost (total transmission power) ratio between the two MTP paths.

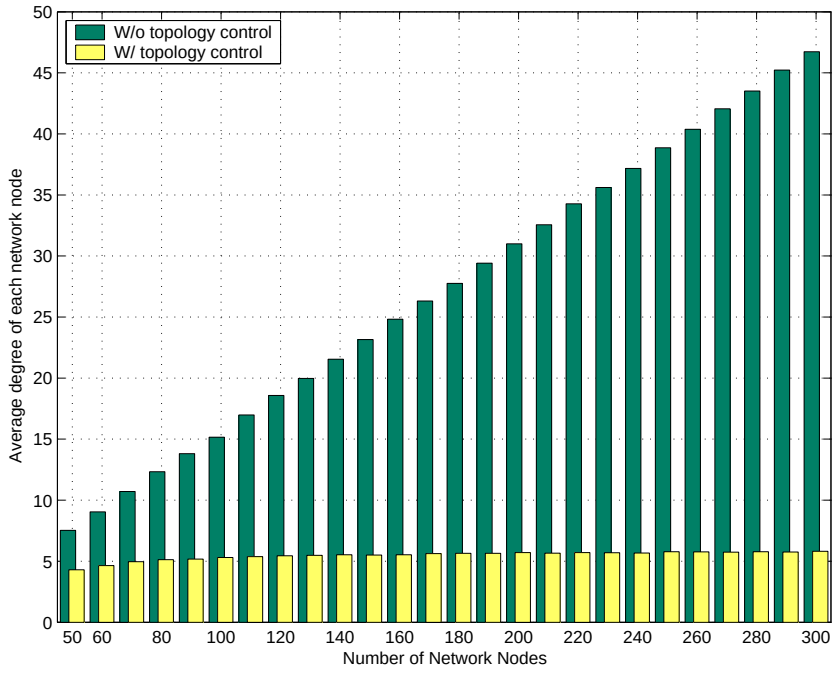


Fig. 20. Average node degree.

While TRUECON preserves the network connectivity, it does not maintain every power efficient path between arbitrary node pairs. Our simulation indicates that the Minimum Transmission Power paths in TRUECON-induced graphs are very close to their counterparts in the original graphs in terms of path length and total cost.

Figs. 26 and 27 depict two networks with 100 and 200 nodes respectively. They show how much TRUECON can reduce the node degree while keeping the network connectivity untouched.

E. Summary

We study the topology control problem of MANETs in a non-cooperative environment. Due to the limited energy reserve of a network node, saving energy is critical to maintain the usability of a MANET. Topology control algorithms allow network

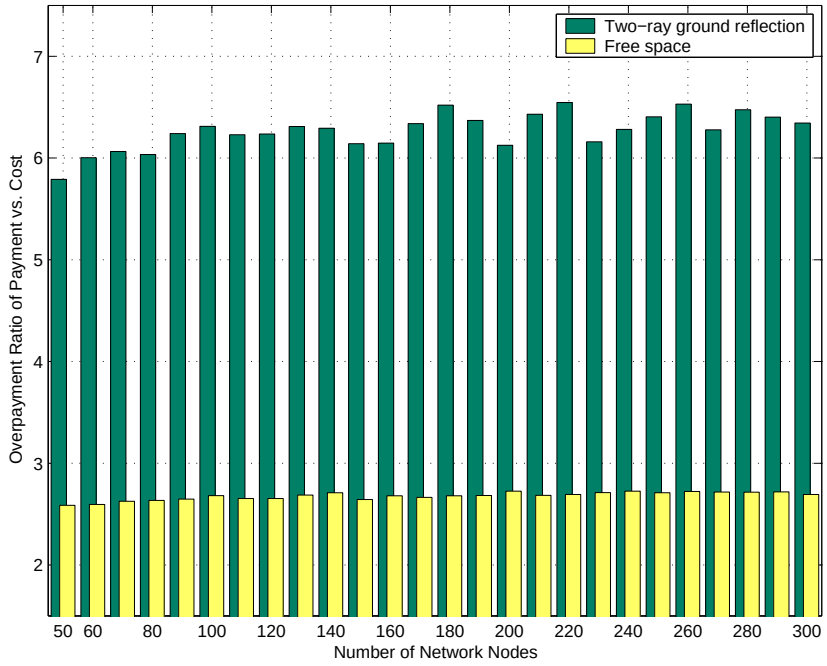


Fig. 21. Overpayment for two different propagation models.

nodes to reduce their transmission power while keeping the same network connectivity as they use the maximum power. However, there is no guarantee on the collaboration among network nodes in MANETs. Forwarding packets for others only incurs energy consumption on intermediate nodes without any obvious benefit. Limited critical resource possession gives an intention to every node to act selfishly.

We propose a truthful topology control mechanism (TRUECON) to attack the selfish intention. TRUECON is a direct-revelation mechanism, in which every node has a quasi-linear utility function. TRUECON belongs to the VCG mechanism family. The truthfulness is proved in this research.

TRUECON can be integrated with ad hoc routing protocols. We revise DSR routing protocol to find a minimum transmission path over the induced network graph. Though the payment along a path must be higher than the actual cost in order to give an incentive to the forwarding nodes, the overpayment has a bound.

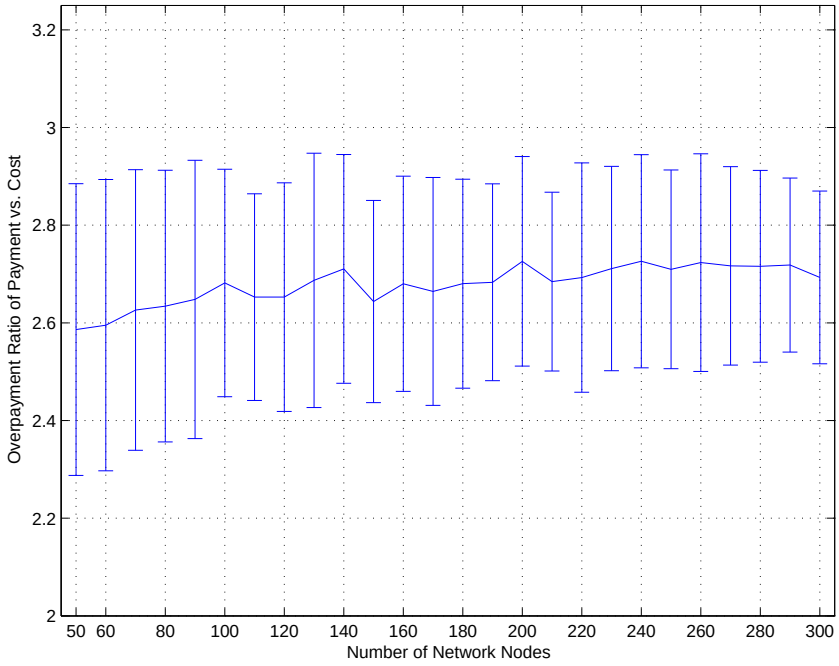


Fig. 22. Overpayment for the free space propagation model.

We prove the bound is only related to the radio path loss exponent. We simulate TRUECON mechanism in different scenarios. The experimental data conforms to our analysis.

TRUECON has its limit in sparse networks. If it is hardly to find replacements for some forwarding nodes, the payment, which is satisfied by both payer and payee, cannot be decided easily. This is also a limit of VCG mechanisms. The impact of node mobility is also worth some future work.

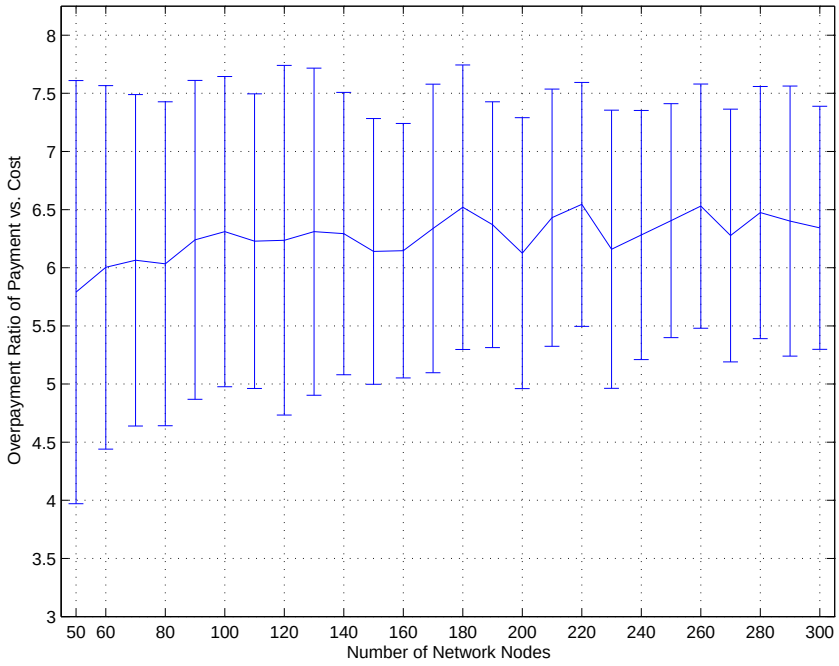


Fig. 23. Overpayment for the two-ray ground reflection propagation model.

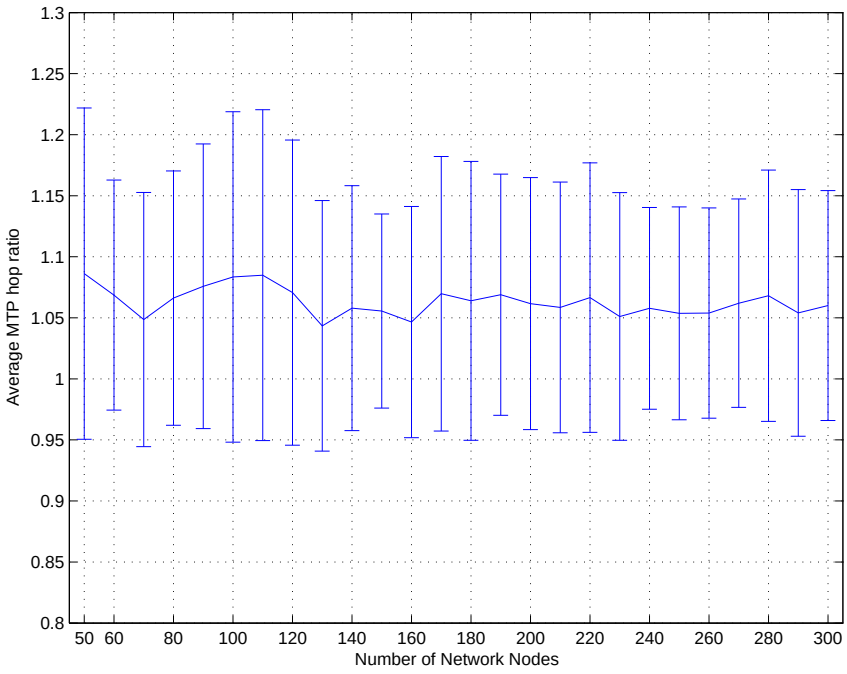


Fig. 24. Normalized length of MTP paths.

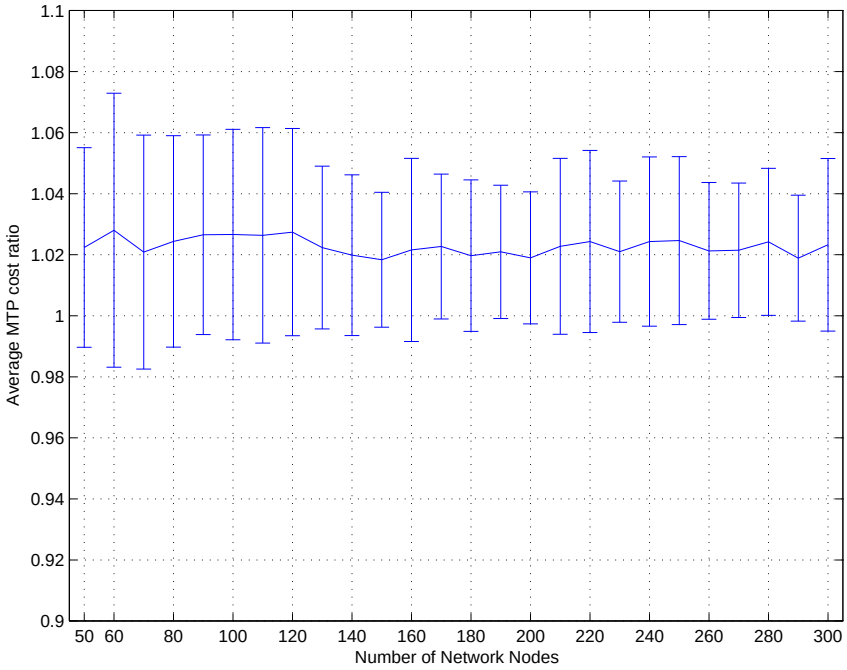
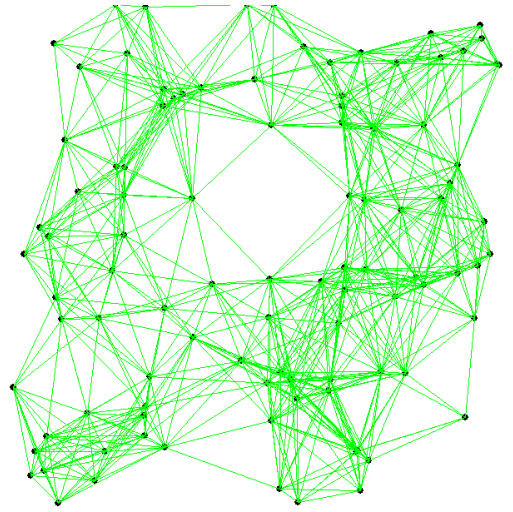
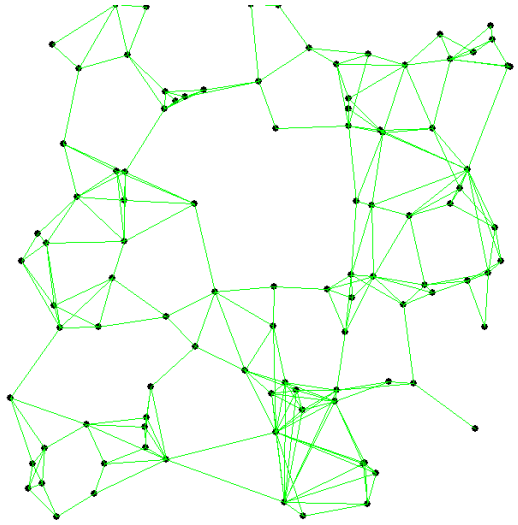


Fig. 25. Cost ratio of MTP paths.

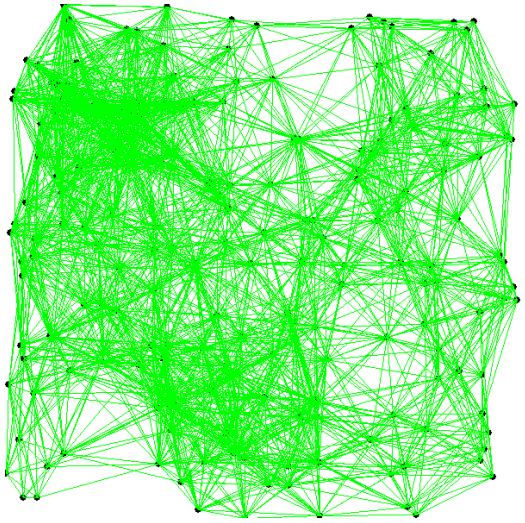


(a)

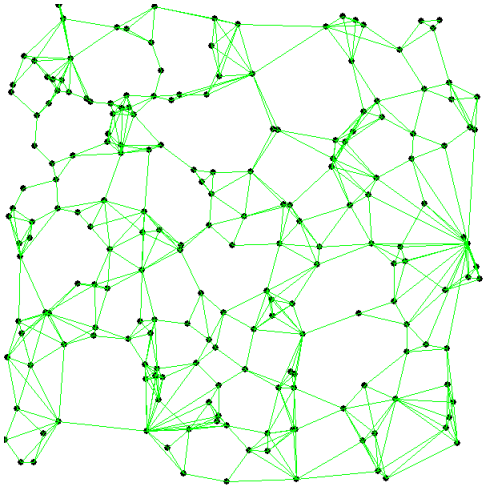


(b)

Fig. 26. Topology control for a network with 100 nodes.



(a)



(b)

Fig. 27. Topology control for a network with 200 nodes.

CHAPTER V

CONCLUSIONS

Wireless mobile ad hoc network (MANET) is a promising communication technology. It can be deployed anywhere and anytime without the dependence on any infrastructures. However the small form factor and limited energy reserve of network nodes pose computation-constraint and resource-constraint to researchers. Energy is the most critical resource in a MANET. In order to prolong the network lifetime, a wealth of research effort has been paid to minimize the energy consumption.

In this dissertation we investigate the resource management problem in MANETs from a game-theoretic approach. A node can be selfish, but it is also rational. Its preference is described as a utility function. The only goal of a rational node is to maximize the outcome of its utility function. We design two truthful mechanisms for network routing and topology control in MANETs.

Anonymity has been studied widely in wired networks. Only little research has been conducted in wireless networks. We extend the definition of being truthful to another level. We consider in some circumstance, a network user tells the truth only when she knows her privacy is protected.

A. Summary of Contributions

We make the following contributions via this research.

1. We propose a truthful routing protocol - Transmission power rEcursive Auction Mechanism routing protocol (TEAM) to deal with selfish nodes. TEAM is a truthful protocol, in which each node has to tell its true value in order to maximize its expected benefit. When come to power efficiency, TEAM approximates

the optimal solution within a bound. Comparing to another truthful routing protocol – Ad-hoc VCG, which needs n^3 messages, TEAM has a much better message complexity – n^2.

2. Truthful topology control is another contribution to non-cooperative MANETs. Based on CBTC algorithm, we design a truthful mechanism – TRUECON to implement the well-known VCG mechanisms from a novel approach. We prove that TRUECON is strategy-proof and preserves the network connectivity. In TRUECON, each node declares its cost for forwarding packets to its neighbors. Its service payment is decided based on its declared value. We show how a routing protocol can be enhanced with TRUECON to find a Minimum Transmission Power path (MTP). Though the payment needs to be higher than the actual total cost of all the nodes, we prove that the overpayment has a bound at 2^{α}, where α is the path loss exponent.

   To our best knowledge, TRUECON is a pioneering work for MANETs. We believe that the non-cooperative character catches the nature of MANETs. As a result, truthful mechanisms are needed at any time when network nodes interact with each other.

3. We conduct a study on enhancement of anonymous communication in MANETs by reducing the transmission power of network nodes. Appendix A presents our study. We propose a routing protocol - Whisper, which can prevent a communication initiator from being revealed in some circumstances. Whisper does not rely on any asymmetric encryption facility, which could be prohibitive to implement on small mobile devices. We obtain some preliminary results of Whisper by simulation.

B. Future Work

In this dissertation, we concentrate on stationary networks, in which network nodes do not move. Though we are confident on that our research works can be validated within a mobile environment, the impacts of node mobility on system performance need future works.

It is observed that though truthful mechanisms can frustrate the selfishness, in a complex network environment, they may not be enough alone. Integrating with other network security techniques, such as cryptographic techniques, we can expect the emergence of more powerful mechanisms to defeat any selfish temptations and achieve the resource efficiency.

REFERENCES

[1] Benjie Chen, Kyle Jamieson, Hari Balakrishnan, and Robert Morris, "Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks.," in *Proc. 7th ACM International Conference on Mobile Computing and Networking*, Rome, Italy, July 2001, pp. 85–96.

[2] J. Gomez, A.T. Campbel, M. Naghshineh, and C.Bisdikian, "Conserving transmission power in wireless ad hoc networks," in *Proc. 9th International Conference on Network Protocols (ICNP2001)*, Riverside, CA, Nov 11-14 2001, pp. 11–14.

[3] Christine E. Jones, Krishna M. Sivalingam, Prathima Agrawal, and Jyh-Cheng Chen, "A survey of energy efficient network protocols for wireless networks," *Wireless Networks*, vol. 7, no. 4, pp. 343–358, 2001.

[4] R. Kravets and P. Krishnan, "Application-driven power management for mobile communication," in *Proc. 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, Dallas, TX, October 1998, pp. 263–277.

[5] Errol L. Lloyd, Rui Liu, Madhav V. Marathe, Ram Ramanathan, and S.S. Ravi, "Algorithmic aspects of topology control problems for ad hoc networks," in *Proc. 3rd ACM International Symposium on Mobile Ad hoc Networking and Computing*, Lausanne, Switzerland, June 2002, pp. 123–134.

[6] Suresh Singh, Mike Woo, and C.S. Raghavendra, "Power-aware routing in mobile ad hoc networks," in *Proc. 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, Dallas, TX, October 1998, pp. 181–190.

[7] Y. Xu, J. Heidenmann, and D. Estrin, "Geography-informed energy conservation for ad hoc routing," in *Proc. ACM/IEEE International Conference on Mobile Computing and Networking*, Rome, Italy, July 2001, pp. 70–84.

[8] Volkan Rodoplu and Teresa H. Meng, "Minimum energy mobile wireless networks," in *Proc. IEEE International Conference on Communications, ICC'98*, Atlanta, GA, June 1998, pp. 1633–639.

[9] Li (Erran) Li and Joseph Y. Halpern, "A minimum-energy preserving topology-control algorithm," *IEEE Transaction on Wireless Communications*, vol. 3, no. 3, pp. 910–921, May 2004.

[10] Roger Wattenhofer, Li (Erran) Li, Victor Bahl, and Yi-Min Wang, "Distributed topology control for power efficient operation in multihop wireless ad hoc networks," in *Proc. IEEE INFOCOM*, Anchorage, Alaska, April 2001, pp. 1388–1397.

[11] R. Ramanathan and R. Rosales-Hain, "Topology control of multihop wireless networks using transmit power adjustment," in *Proc. IEEE INFOCOM*, Tel-Aviv, Israel, March 2000, pp. 404–413.

[12] Alberto Cerpa and Deborah Estrin, "Ascent: Adaptive self-configuring sensor networks topologies," *IEEE Transactions on Mobile Computing Special Issue on Mission-Oriented Sensor Networks*, vol. 3, no. 3, pp. 272–285, July 2004.

[13] S. Singh and C. S. Raghavendra, "Pamas: Power aware multi-access protocol with signalling for ad hoc networks," *ACM Computer Communication Review*, vol. 28, no. 3, pp. 5–26, July 1998.

[14] Xiang-Yang Li, Peng-Jun Wan, Yu Wang, and Chih-Wei Yi, "Fault tolerant

deployment and topology control in wireless networks," in *Proc. 4th ACM international symposium on Mobile ad hoc networking and computing*, Annapolis, MD, June 2003, pp. 117–128.

[15] Xiang-Yang Li and Yu Wang Wen-Zhan Song, "Efficient topology control for ad-hoc wireless networks with non-uniform transmission ranges," *ACM WINET*, 2003.

[16] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, Boston, MA, August 2000, pp. 255–265.

[17] Seung Yi, Prasad Naldurg, and Robin Kravets, "Security-aware ad hoc routing for wireless networks," Tech. Rep. UIUCDCS-R-2001-2241, Department of Computer Science, University of Illinois at Urbana-Champaign, August 2001.

[18] Lidong Zhou and Zygmunt J. Haas, "Securing ad hoc networks," *IEEE Network Magazine*, vol. 13, no. 6, pp. 24–30, Nov/Dec 1999.

[19] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, and Elizabeth M. Belding-Royer, "A secure routing protocol for ad hoc networks," in *Proc. 10th IEEE International Conference on Network Protocols (ICNP 2002)*, Paris, France, November 2002, pp. 78–89.

[20] Levente Buttyan and Jean-Pierre Hubaux, "Nuglets: a virtual currency to stimulate cooperation in self-organized mobile ad hoc networks," Tech. Rep. DSC/2001/001, School of Computer and Communication Sciences, Swiss Federal Institute of Technology, Lausanne, Swiss, January 2001.

[21] N. Salem, L. Buttyan, J. Hubaux, and M. Jakobsson, "A charging and rewarding scheme for packet forwarding in multi-hop cellular networks," in *Proc. of the 4th ACM/SIGMOBILE MobiHoc*, Annapolis, MD, June 2003, pp. 13–24.

[22] Luzi Anderegg and Stephan Eidenbenz, "Ad hoc-vcg: a truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents," in *Proc. 9th Annual International Conference on Mobile Computing and Networking*, San Diego, CA, Sep 2003, pp. 245–259.

[23] Jianfeng Cai and Udo Pooch, "Play alone or together - truthful and efficient routing in wireless ad hoc networks with selfish nodes," in *Proc. 1st IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS'04)*, Fort Lauderdale, FL, October 2004, pp. 457–465.

[24] Stephan Eidenbenz, Giovanni Resta, and Paolo Santi, "Commit: A sender-centric truthful and energy-efficient routing protocol for ad hoc networks with selfish nodes," in *Proc. 5th IEEE International Workshop on Algorithms for Wireless, Mobile, Ad Hoc and Sensor Networks (WMAN 05)*, Denver, CO, April 2005.

[25] Jianfeng Cai and Udo Pooch, "Allocate fair payoff for cooperation in wireless ad hoc networks using shapley value," in *Proc. 4th International Workshop on Algorithms for Wireless, Mobile, Ad Hoc and Sensor Networks (WMAN)*, Santa Fe, NM, April 2004, Proceedings in CD ROM.

[26] David B. Johnson and David A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing*, Tomasz Imielinski and Hank Korth, Eds. Dordrecht, The Netherlands: Kluwer Academic Publishers, 1996, pp 153-181.

[27] L.C. Thomas, *Games, Theory and Applications*, Chichester, UK: Ellis Horwood Limited, 1984.

[28] Prajit K. Dutta, *Strategies and Games: Theory and Practice*, Cambridge, MA: MIT Press, 1999.

[29] David C. Parkes, "Iterative combinatorial auctions: Achieving economic and computational efficiency," Ph.D. dissertation, Computer and Information Science, University of Pennsylvania, Philadelphia, May 2001.

[30] John Nash, "Equilibrium points in n-person games," in *Proc. National Academy of Sciences*, 1950, vol. 36, pp. 48–49.

[31] William Vickrey, "Counterspeculation, auctions, and competitive sealed tenders," *The Journal of Finance*, vol. 16, no. 1, pp. 8–37, Mar. 1961.

[32] E. H. Clarke, "Multipart pricing of public goods," *Public Choice*, vol. 11, pp. 17–33, 1971.

[33] Theodore Groves, "Incentives in teams," *Econometrica*, vol. 41, no. 4, pp. 617–631, July 1973.

[34] Jerry R Green and Jean-Jacques Laffont., "Characterization of satisfactory mechanisms for the revelation of preferences for public goods," *Econometrica*, vol. 45, pp. 427–438, 1977.

[35] Theodore S. Rappaport, *Wireless Communication: Principles and Practice*, Upper Saddle River, NJ: Prentice Hall, 1996.

[36] Laura M. Feeney and Martin Nilsson, "Investigating the energy consumption of a wireless network interface in an ad hoc networking environment," in *Proc. IEEE INFOCOM*, Anchorage, AK, April 2001, pp. 1548–1557.

[37] S. Zhong, Y. R. Yang, and J. Chen, "Sprite: A simple, cheat-proof, credit-based system for mobile ad hoc networks," in *Proc. INFOCOM 2003*, San Francisco, CA, March 2003, pp. 1987–1997.

[38] John Dorsey, "Game-theoretic power management in mobile ad hoc networks," Ph.D. dissertation, Electrical and Computer Engineering, Pittsburgh, PA, Carnegie Mellon University, August 2001.

[39] Joan Feigenbaum, Christos Papadimitriou, and Scott Shenker, "Sharing the cost of multicast transmissions," *Journal of Computer and System Sciences*, vol. 63, no. 1, pp. 21–41, Aug. 2001.

[40] Joan Feigenbaum and Scott Shenker, "Distributed algorithmic mechanism design: recent results and future directions," Invited talk in DIAL-M'02, Atlanta, GA, Sep 2002.

[41] Tim Roughgraden, "How unfair is optimal routing," in *Proc. Thirteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, San Francisco, CA, Jan 2002, pp. 203–204.

[42] N. Nisan and A. Ronen, "Algorithmic mechanism design," *Games and Economic Behavior*, vol. 35, pp. 166–196, 2001.

[43] Charles E. Perkins and Elizabeth M. Royer, "Ad hoc on-demand distance vector routing," in *Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications*, New Orleans, LA, February 1999, pp. 90–100.

[44] "The network simulator - ns-2," June 2005, Information Sciences Institute, the University of Southern California, http://www.isi.edu/nsnam/ns/.

[45] "Wireless and mobility extensions to ns-2," June 2005, the Rice Monarch Project, http://www.monarch.cs.rice.edu/cmu-ns.html.

[46] P. Gupta and P. R. Kumar, "The capacity of wireless networks," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 388–404, March 2000.

[47] Jinyang Li, Charles Blake, Douglas S. J. De Couto, Hu Imm Lee, and Robert Morris, "Capacity of ad hoc wireless networks," in *Proc. 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom)*, Rome, Italy, July 2001, pp. 61–69.

[48] Li (Erran) Li, Joseph Y. Halpern, Victor Bahl, Yi-Min Wang, and Roger Wattenhofer, "Analysis of a cone-based distributed topology control algorithms for wireless multi-hop networks," in *Proc. ACM Symposium on Principle of Distributed Computing (PODC)*, Newport, RI, August 2001, pp. 264–273.

[49] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein, *Introduction to Algorithms*, Cambridge, MA: MIT Press, second edition, 2001.

[50] *Data Protection Act 1998*, the Queen's Printer of Acts of Parliament, June 2005, http://www.hmso.gov.uk/acts/acts1998/19980029.htm.

[51] D. Goldschlag, M. Reed, and P. Syverson, "Onion routing for anonymous and private internet connections," *Communications of the ACM*, vol. 42, no. 2, pp. 39–41, Feb. 1999.

[52] P. Syverson, D. Goldschlag, and M. Reed, "Anonymous connections and onion routing," in *IEEE Symposium on Security and Privacy*, Oakland, California, May 1997, pp. 44–54.

[53] P. Syverson, M. Reed, and D. Goldschlag, "Onion routing access configuration," in *Proc. DARPA Information Survivability Conference and Exposition*, Hilton Head, SC, January 2000, pp. 34–40, IEEE CS Press.

[54] Jiejun Kong and Xiaoyan Hong, "Anodr: Anonymous on demand routing protocol with untraceable routes for mobile ad-hoc networks," in *Proc. 4th ACM international symposium on Mobile ad hoc networking and computing*, Annapolis, MD, June 2003, pp. 291–302.

[55] "Anonymizer," June 2005, Anonymizer, Inc., http://www.anonymizer.com/.

[56] David Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–88, Feb. 1981.

[57] Michael Reiter and Aviel Rubin, "Crowds: Anonymity for web transactions," *ACM Transactions on Information and System Security*, vol. 1, no. 1, pp. 66–92, June 1998.

[58] Hongfei Sui, Jianxin Wang, Jianer Chen, and Songqiao Chen, "The cost of becoming anonymous: on the participant payload in crowds," *Information Processing Letters*, vol. 90, no. 2, pp. 81–86, April 2004.

[59] Luis von Ahn, Andrew Bortz, and Nicholas J. Hopper, "k-anonymous message transmission," in *Proc. 10th ACM conference on Computer and communication security*, Washington, DC, Oct 2003, pp. 122–130.

[60] Yong Guan, Xinwen Fu, Riccardo Bettati, and Wei Zhao, "A quantitative analysis of anonymous communications," *IEEE Transactions On Reliability*, vol. 53, no. 1, pp. 103–116, March 2004.

APPENDIX A

A STUDY OF ANONYMITY IN MANETS

1. Introduction and Motivation

Privacy is a human right protected in both real world and cyberspace. In many researches, keeping data as anonymous as possible is the prerequisite for conducting experiments on people. Since the introduction of the British Data Protection Act (1998) [50], anonymity is not only an ethical issue, but also a legal implication. In the Internet, anonymous communication is demanded in many applications, such as E-voting systems and web transactions, etc. Anonymity in mobile ad-hoc networks (MANETs) has not draw much attention yet because of the relatively short history of this research area. However, with more and more emerging applications of MANETs, anonymity poses a concern to network design and configuration.

A wealth of anonymous systems has been proposed for wired networks. They address the different network environments, making them difficult to migrate to the highly dynamic ad-hoc context. For example, Onion [51, 52, 53] is a successful anonymous system in wired networks. It is not only able to conceal the sender from the recipient but also to hide correlation between a sender and its recipient. However it needs a centralized server and uses asymmetric encryption mechanisms, which are either impractical or too costly to be implemented in MANETs.

A sound solution of anonymity in MANETs can be found in ANODR [54], in which data packets are encrypted hop by hop like an onion structure. However, it bans the IDs in any data transmission, which results in lack of compatibility with most of the existing routing and MAC protocols.

Due to the limited energy and computational ability, the widely used public key mechanism is extremely expensive to be applied in MANETs. With consideration of the characteristics of MANETs, we propose Whisper routing protocol to enhance anonymity protection of the initiator or source node. The initiator anonymity is considered most critical in many applications, comparing to the destination anonymity and initiator/destination linkability. Whisper is compatible to the current fully-fledged MAC layer protocols.

In whisper, a topology control algorithm, such as CBTC [48], is run by each node before the routing takes place. A node sends a Route Request packet to its nearest neighbor with a probability p_f or starts a route discovery with a probability $1 - p_f$. A forwarding node replaces the source ID in the packet with its own ID. Therefore the intermediate nodes act as proxies for finding a path from the source to the destination.

In MANETs, eavesdroppers can be more effective than in wired networks. They do not have to be chosen as a router on the transmission path while overhearing all the data packets of its neighbors. Whisper lets nodes use the minimum transmission power to talk to their nearest neighbors. Consequently, the number of nodes exposed to the passive attackers is reduced dramatically, especially in a dense network. Reducing transmission power can also save energy and decrease the radio interference.

The remainder of Appendix A is organized as follows: Section 2 gives a brief review on related work. The threat model is described in Section 3. Section 4 presents the design of Whisper. Section 5 discusses attacking and counterattack strategies. Simulation results and analysis can be found in Section 6 and Section 7 concludes.

2. Related Work

Anonymous communication has been studied extensively in the environment of wired networks. Anonymizer [55] is a web proxy providing anonymous communication services for web clients in a network. It filters out the service requester's identity information contained in the header and replaces it with the identity of the Anonymizer-server. All messages can only be traced back to the server after they go through it. Therefore the real web clients are protected. This scheme is simple and easy to be applied. However, as the only intermediate node, the Anonymizer-server is apt to be the target and becomes the single failure point. Moreover, the scheme is not scalable to network growth since the payload of the Anonymizer-server increases linearly with the network size.

A mix [56] is an enhancement of the proxy-based scheme. It collects messages with fixed length from different sources, cryptographically transforms these messages, and sends them to their recipients in a different order. It is further developed as Onion-routing schemes in [51, 52, 53]. In Onion-routing schemes, there is an onion-router network, in which each onion-router works like a mix. A sender chooses a sequence of onion-routers as the rerouting path. The path can be reused for a period. Each message passes through the sequence of onion-routers before it reaches the recipient. Onion not only hides a sender from its recipient, but also prevents global eavesdroppers from linking the sender with the recipient. However, the schemes are not scalable using a fixed number of onion-routers. Since there are no centralized servers in ad-hoc networks working as onion-routers, the schemes cannot be applied in ad-hoc networks directly.

Crowds [57] is a well known anonymous communication protocol to protect Internet transactions. The intuition of Crowds is to hide the communication in crowds.

A member of the Crowds forwards service requests and data for others. Eavesdropping cannot help to identify the initiator of a data request if it intercepts a packet in the middle. Different anonymous degrees are defined as from "absolute anonymous" to "provable exposed". Crowds can achieve possible innocence in the presence of c collaborators, which are snooping the network traffic and try to locate the initiator, if the Crowds has n members and n satisfies

$$n \geq \frac{p_f}{p_f - \frac{1}{2}}(c+1)$$

Sui et al. [58] prove the participant payload in Crowds does not depend on the size of the crowd and its expected value is $\frac{1}{1-p_f} + 1$.

ANODR [54] is a complete solution for anonymity in ad-hoc networks using encryption facilities. The identities of network nodes are banned in each network protocol layer. A sender in ANODR chooses the routing path like regular AODV routing protocol, but messages are encrypted by every intermediate node like an onion. Only the recipient can open the "trap-door" in the message and know it is the destination of the message. This scheme gains full anonymity even under global eavesdropping. However, the absence of IDs poses challenges for the protocol implementation and limits its applications.

[59] proposes the concept of k-anonymous and its applications. They also present a simple and efficient communication protocol, in which an adversary is only able to narrow down the suspicious sender or receiver to a set of k nodes.

3. Threat Model

A source node (or an initiator) is the start of a path. A destination node is the end of a path. There are three types of anonymity to achieve:

- Initiator anonymity. The identity of the initiator needs to be prevented from being revealed.

- Destination anonymity. The ID of the intended destination should be prevented from being revealed.

- Initiator-destination linkability. If an attacker observes a series of initiators and destinations but cannot figure out whether they are related by all means, we say the anonymity of initiator-destination linkability is achieved.

From the research results in the past, we know that the initiator anonymity is the most important in many cases. Enhancing the initiator anonymity protection in MANETs is the motivation of this study.

In a wireless network, network traffic is transferred in the open medium - air. If a node v_i is within the communication range of another node v_j, then i can overhear all the packets v_j sends out even though they are not addressed to v_i. Due to the design of routing protocols, a packet usually contains the identities of the source node, the destination node, and the forwarding node of each hop. Therefore even if we encrypt the content of a packet, the routing information stored in the packet header is still vulnerable to passive anonymity attackers who want to identify the initiator.

We define three different attack scenarios:

- A *local attacker* is always able to overhear all the traffic of its neighbors. It tries to figure out which node is the initiator based on the intercepted packets. A compromised initiator is also in this category.

- Attackers may collaborate with each other and exchange information in order to solve the puzzle by correlating all the clues caught locally. Each collaborating attacker is a *collaborator*. Please note that if there are multiple attackers in a

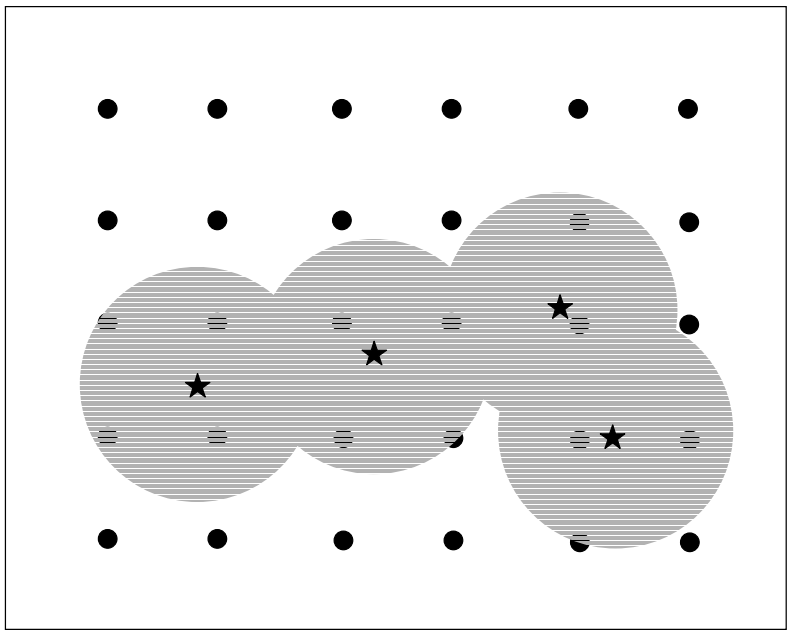


Fig. 28. The stars are the collaborators who are monitoring the dark area to locate an initiator.

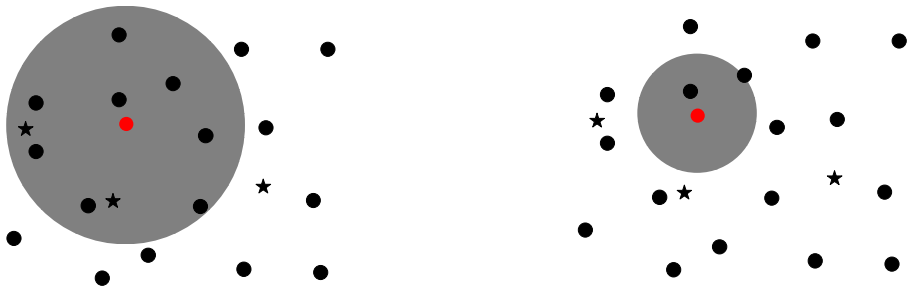
MANET but they never talk to each other, we regard them as a set of local attackers.

- An *end server attacker* is the destination node, which could be a server receiving service requests.

In a MANET, each passive attacker can monitor its vicinity, collaborate and exchange information with other attackers. Fig 28 shows the scenario, in which a group of such attackers collaborate to eavesdrop the network and try to pinpoint the initiator.

4. Design of Whisper

In a MANET, each node may act as a router to serve others in order to fulfill the network function. Then the network nodes form a pool of forwarding routers like Crowds [57]. In contrast to ANODR [54], we preserve the node IDs in a packet



(a) (b)

Fig. 29. The stars are nodes eavesdropping on network traffic. The center node of the shadow area is a source node, which initiates a communication session. (a)When the sending node communicates at high power level, it is likely to be overheard by at least one of the eavesdroppers. (b)The sending node reduces its transmission power to avoid the eavesdroppers.

though the value of the source ID in a packet is changed hop by hop along the Whisper path. The definition of a *Whisper path* is given later in this section. We assume that every node knows its location and broadcasts the information with Hello messages periodically. Hence, each node knows its neighbors' IDs and locations.

In Whisper, a source node S transfers (whispers) a Route Request (RREQ) packet to its nearest neighbor v_1 with a probability p_f using the minimum transmission power. Or it starts a Route Discovery with a probability $1 - p_f$. Upon receiving a RREQ, v_1 make its choice between forwarding the packet to the nearest neighbor and initiating a route discovery with the same probability as S. This process repeats at each forwarding node as long as every node chooses sending to its nearest neighbor.

If a node decides to relay the packet to its nearest neighbor, it always excludes the node, from which the packet comes. After locating the nearest neighbor, the forwarding node replaces the source ID in the packet with its own ID. When a node

v_i finally decides to start a route discovery process, it uses an AODV-like routing protocols to find a path. From then on, the ID of the source node in the packet remains unchanged as v_i.

On a path from S to D, the part between S and v_i is called *Whisper path* and the part after v_i until D is called *normal path*. A path is expressed as a series of node IDs. Then the Whisper path is $\sigma_{Whisper}\{S, n_1, n_2, \ldots, n_i\}$. Node n_i is the last node on Whisper path and the first one on normal path. The normal path is described as $\sigma_{normal}\{n_i, \ldots, n_l = D\}$, where $l > i$.

Due to the characteristic of radio propagation, the received signal strength P_r can be expressed as

$$P_r = \frac{K \times P_t}{d^\alpha}$$

where K is a constant and α is a number between 2 and 6 [35]. If P_r is greater than a threshold P_{thd}, the data can be received successfully by the receiver, otherwise the data is lost. Since a node can adjust the transmission power of its radio component, the communication area can be refined within a certain range. Whisper lets nodes use the minimum power to forward packets to its nearest neighbor, therefore the number of overhearing nodes along the Whisper path is reduced to minimum. Fig 29 shows the effect of various transmission power used by a sending node.

If an attacker is in the communication range of an initiator, it can always locate it by analyzing the observed traffic pattern. An intermediate node may receive a packet first, then sends out a packet later on. The initiator usually has no incoming traffic before it sends the first packet. To deal with this special case, we let the MAC layer be involved. For example, in 802.11 protocol, a pair of RTS (Request-To-Send) and CTS (Clear-To-Send) are exchanged between sending and receiving nodes. To imitate this process, we let the initiator send a CTS, followed by an Ack (Packet

Acknowledgment) after a short time period. From the neighbor's point of view, this is a typical packet receiving procedure. Then a neighbor believes the real initiator has received a packet from another node, even when the RTS is not heard. Due to the hidden terminal problem, not hearing incoming packets happens frequently while the overhearing node and the sending node reside on different side of the receiving node.

An attacker can figure out this trick only in following cases.

- The node with the inserted ID in the CTS does not exist in the network. This requires the full knowledge of a network. In a MANET, a node can join and leave the network at any time thus it is non-trivial to get this knowledge.
- The inserted ID belongs to a collaborator or a node from which the attacker can get a proof on whether it does the communication.

Based on the observation, we can let an initiator only insert the ID of a trustable node in the network. And that node never answers any inquiry about its communication sessions.

5. Analysis of Whisper

In this section, we analyze the strategies of passive attackers and show how the anonymity is enforced in MANETs with Whisper.

a. Strategies of Passive Attackers

We adopt the method in [60] to analyze the strategies used by passive attackers which are collaborating with each other. Suppose that there are M attackers in a MANET, and the attackers know the forwarding path selection algorithm and related parameters (e.g. p_f). We denote the attackers (or collaborators) as a set

of compromised nodes, $\{C_1, C_2, \ldots, C_i, \ldots, C_M\}$. When an attacker C_i overhears a message, it records the event in the format of $< t_{C_i}, P_{C_i}, C_i, S_{C_i}, Q_{C_i} >$, where t_{C_i} is the time when the message is heard; P_{C_i} is the sender in this hop; S_{C_i} is the receiver in this hop, and Q_{C_i} is the set of nodes that can be excluded from the set of possible initiators by C_i. If C_i does not hear anything, it just generates a report as $< t_{C_i}, C_i, Q_{C_i} >$ to indicate nothing happens around it. The collaborators exchange their reports and sort them by the order of t_{C_i}. They try to find out the initiator based on the partially identified path. To determine a set of possible initiators, the collaborators construct a node set NS including all of the nodes, which are impossible to be the initiator, according to the reports. The rules of NS construction are listed in Table V.

If L' is the maximum path length of any route from the source S to the destination D, the attackers can always confidently remove those nodes that are farther than L' hops away from the spot of the overheard communication. It is because that the communication range of a network node is limited. However this requires the collaborators to have the full knowledge of the network topology, which is dynamically changing.

After information collection, the collaborators attempt to find out which node is more likely to be the real initiator among the set of possible nodes. The probability of P_{C_1} being the initiator is denoted as

$$Pr\{S = P_{C_1} | F = w\} = \frac{Pr\{S = P_{C_1}, F = w\}}{P(F = w)} \quad (A.1)$$

$$= \frac{\sum_{k=|N_i|}^{\infty} p_f^k (1 - p_f) \frac{1}{k - |N_i| + 1}}{P(F = w)} \quad (A.2)$$

S is the identified initiator; F denotes the facts that the collaborators collected;

Table V. NS CONSTRUCTION RULES

Rule	Pre-condition	Action
R1	(P_{C_1}= NULL) and ($S_{C_1} \neq$ NULL)	NS:=NS $\cup$ ($V \backslash \{C_1\}$)
R2	($P_{C_1} \neq$ NULL) and the partial path from C_1 to R is completely identified and the path length is L'	NS:=NS $\cup$ ($V \backslash \{P_{C_1}\}$)
R3	$\forall C_i \in$ CNH	NS:=NS $\cup \{C_i\} \cup \{Q_{C_i}\}$
R4	$\forall k > 1, C_k \in$ CH	NS:=NS $\cup \{C_k, P_{C_k}, S_{C_k}\} \cup \{Q_{C_k}\}$
R5	$P_{C_1} \neq$ NULL	NS:=NS $\cup \{C_1, S_{C_1}\} \cup \{Q_{C_1}\}$
R6	($P_{C_1} \neq$ NULL) and the partial path from C_1 to R is completely identified and the path length is less than L'	NS:=NS $\cup \{P_{C_1}\}$
R7	$L > 0$	NS:=NS $\cup \{D.P\}$

Notations:

CNH	a set of attackers which overhear nothing
CH	a set of attackers which overhear messages
V	a set of all nodes in the network
L	path length
L'	guessed path length by the adversary
$D.P$	immediate predecessor of the message receiver

w is the reports generated by the attackers; n is the number of network nodes; k is the path length and $|N_i|$ represents the number of nodes, which cannot be the initiator. (A.2) is the sum of the probabilities of that P_{C_i} is the initiator, given the path length as k. The product of the first two terms is the probability of a k-hop path. The third term is the probability of P_{C_1} being the initiator, given the path length.

If P_{C_1} is not an initiator, all other nodes, which cannot be eliminated, have the same probability to be the initiator. We have

$$Pr\{S = s|F = w\} = \frac{1 - Pr\{S = P_{C_1}|F = w\}}{n - |NS| - 1} \tag{A.3}$$

s denotes the true sender.

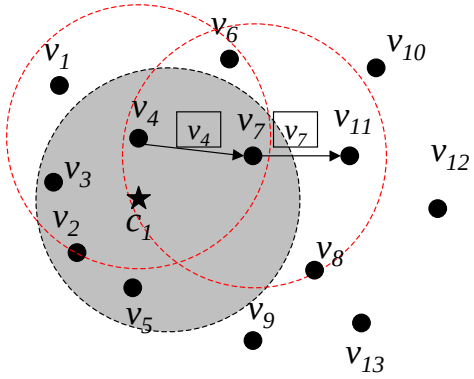
b. Strategies of Protecting Anonymity with Whisper

We let the coverage area of a MANET be σ and a node's transmission range be R. We model the communication region as a Unit Disk Graph (UDG). Thus $\sigma = \pi R^2$.

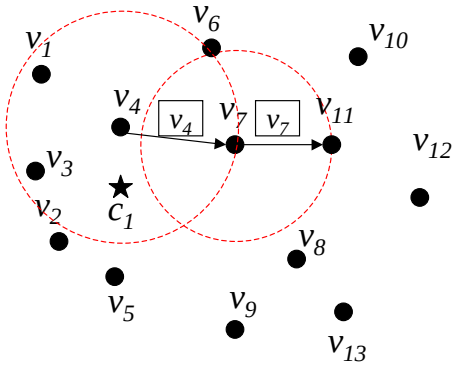
The node density in an area S_a is $\frac{n}{S_a}$. Then the expected neighbor number of a sender is $\pi R^2 \frac{n}{S}$. If there are c collaborators in the whole area, then the number of collaborators in the transmission area of sending node is $\pi R^2 \frac{c}{S_a}$. If c and S_a are fixed, the smaller the transmission range, the less the probability of the sending node being captured by any attacker. If this value is less than 1, we would say a transmission is not likely to be overheard by even one attacker.

Obviously, if the collaborators can eliminate more nodes from the set of possible initiators, they have higher probability to identify the true initiator. From NS construction rules in Table V, we can find that how to get Q_{C_i} becomes the key issue for the collaborators to make a good guess. An adversary derives $Q_{C_i} = N_{C_i} - P_{C_i}$, where N_{C_i} is the set of nodes that C_i can overhear from. If every node is required to send messages with high transmission power in a MANET where the nodes are evenly

distributed, it can be approximated that $|N_{C_i}| = n\frac{\pi R^2}{S}$. If a node only send messages to its nearest neighbor with minimum power, an adversary can only approximate N_{C_i} as the set of nodes within the transmission range r, where r is the average distance between two adjacent nodes in the network. In this case, $|N_{C_i}|$ can be approximated as $n\frac{\pi r^2}{S}$. Clearly, in a non-sparse MANET, after every node reducing its transmission power, an attacker can eliminate much less nodes from possible initiators. It results in a much worse guess of the collaborators.



(a)



(b)

Fig. 30. A MANET with 15 nodes including attacking node C_1.

For example, we have a MANET as Fig.30 shows. We assume the messages are transmitted with the maximum power level. C_1 generates $< t^1_{C_1}, v_4, C_1, v_7, \{v_2, v_3, v_5\} >$ and $< t^2_{C_1}, v_7, C_1, v_{11}, \{v_2, v_3, v_5\} >$ since it overhears messages sent from both v_4 and v_7. Then NS=$\{v_2, v_3, v_5, v_7, C_1\}$ and

$$\begin{aligned} Pr\{S = v_4 | F = w\} &= \frac{0.75 \times 0.25 + 0.75^2 \times 0.25 \times \frac{1}{2} + \ldots}{1 - 0.25 - 0.75 \times 0.25} \\ &= 0.6161 \end{aligned}$$

If v_4 is not the initiator, the probability that the collaborators can identify the true initiator is

$$\begin{aligned} Pr\{S = s | F = w\} &= \frac{(1 - Pr\{S = v_4 | F = w\})}{15 - 5 - 1} \\ &= 0.0427 \end{aligned}$$

If the packet is transmitted using reduced power, C_1 reports its overhearing result as $< t_{C_1}, v_4, C_1, v_7, \{NULL\} >$. C_1 cannot eliminate any node except itself, then NS=$\{C_1\}$. Then,

$$\begin{aligned} Pr\{S = v_4 | F = w\} &= \frac{0.75 \times 0.25 + 0.75^2 \times 0.25 \times \frac{1}{2} + \ldots}{1 - 0.25} \\ &= 0.4592 \end{aligned}$$

If v_4 is not the initiator,

$$\begin{aligned} Pr\{S = s | F = w\} &= \frac{(1 - Pr\{S = v_4 | F = w\})}{15 - 1 - 1} \\ &= 0.0416 \end{aligned}$$

It shows that when messages are transmitted with the reduced power, the collab-

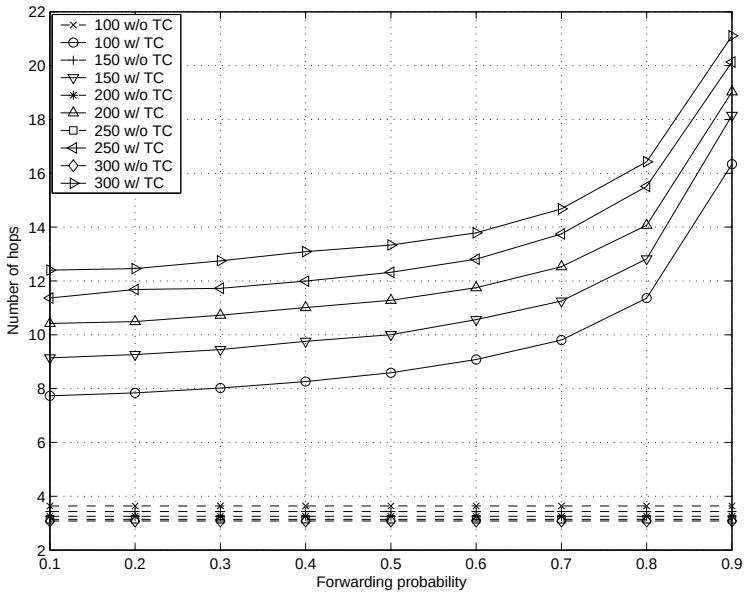


Fig. 31. Path length versus forwarding probability.

orators have lower probability to identify the real initiator. This justifies the scheme of reducing transmission power in Whisper.

Since in a MANET a node can move while overhearing the neighborhood, the communication session should not last long enough for an attacker tracking back from the destination to the source node.

6. Simulation

We simulate Whisper using ns-2 network simulator [44]. Every node has a radio with 2Mbps bandwidth and 150-meter communication range. We simulate the networks in a 600m $\times$ 600m area, in which we set the node number as 100, 150, 200, 250 and 300. Nodes are stationary and put into the area uniformly. We assume each node knows its own location from some positioning services, such as GPS. The location information is broadcast in Hello messages periodically. The source node and destination node are put on the different sides of the network area. There is a topology control algorithm

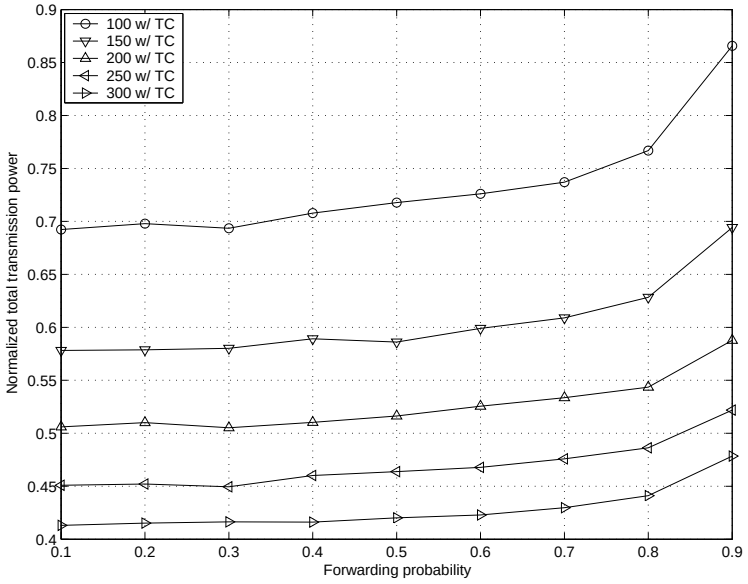


Fig. 32. Normalized power consumption over a path.

run by every node before the routing takes place.

Whisper runs as a routing protocol over the network layer. The source node tosses a bias coin, which has a probability Pf in favor of head. If the result is head, then it sends a Route Request to its nearest neighbor. Otherwise, it starts a Route Discovery. The receiving neighbor also needs to make a decision on forwarding to the nearest neighbor, except its predecessor, or initiating a Route Discovery. The same procedures are taken at the following nodes until a tail comes up. We vary the forwarding probability as 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8 and 0.9. The route length, the aggregate transmission power and the number of node hearing the communication are measured.

As references, we simulate the networks, in which every node transmits using the maximum power, for the same scenarios as Whisper. In these networks, nodes run AODV to discover a path from the source to the destination and the forwarding probability is zero. In another word, a source always initiates a route discovery. Thus

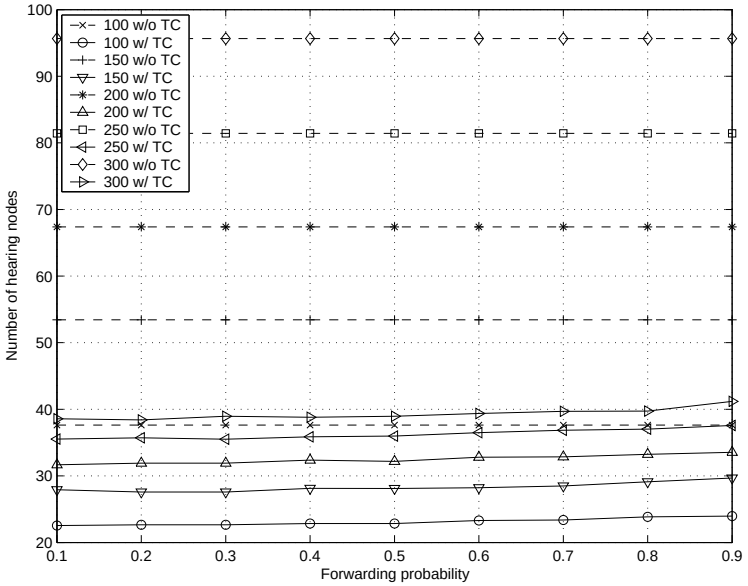


Fig. 33. Number of hearing nodes versus forwarding probability.

the result data of these networks is always displayed as straight lines in the figures.

We plot the simulation results in Fig. 31, 32, 33. Each point in the figures is the average value of 1000 runs. Fig. 31 shows, in hops, the length of a path between the source node and the destination node. Fig. 32 presents the ratio of the aggregate transmission power on a path discovered by Whisper with power control and that on an AODV path without power control. Fig. 33 displays the number of the node, which can hear the Route Request packet.

We observe that route length increases as the forwarding probability rises. With a high forwarding probability, the neighbor is very likely to forward the Route Request to its nearest neighbor rather than start finding a path to the destination. Therefore, the total path length is longer at high forwarding probability than at low forwarding probability.

Because we integrate the topology control technology with Whisper, a node usually finds a path with more hops than routing without topology control. Fig. 32 shows

that the short-distance-hop path of Whisper consumes less transmission power than the AODV path with nodes sending at the maximum power. This result complies with our discussions in Chapter IV.

Fig. 33 shows the number of nodes, which are able to hear the communication. These nodes include the intermediate forwarding node and those within the communication range of the sending nodes. If an attacker is among these nodes, it may collect as much information as possible in order to figure out who is the initiator. The less these hearing nodes, the smaller the probability they include attackers. While reducing the transmission power of each node, the communication is confined within a much smaller set of nodes. This is a desirable property for protecting anonymity in MANETs. The hearing node number increases with the node density.

7. Summary

Anonymous communication has been studied intensively in the wired network environment while little work is done for MANETs. Due to the limited computation capacity of network nodes, anonymous communication protocols designed for wired networks are not suitable for MANETs. We propose Whisper - a routing protocol to enhance initiator anonymity in MANETs by reducing transmission power.

In Whisper, a sender transmits messages to its nearest neighbor node with reduced power by a certain probability. Whisper does not rely on public key facilities. Attacking and protecting strategies are analyzed. We show that in certain scenarios, a passive attacker is more difficult to find the real initiator in a MANET with Whisper than without.

Simulation results confirm that Whisper incurs less power consumption and smaller hearing node sets than routing protocols without any intention to control the transmission power of network nodes.

APPENDIX B

NETWORK SIMULATION

In this dissertation, we simulate MANETs using ns-2 network simulator [44] with the wireless extension of Monarch project [45]. The MAC layer protocol is IEEE 802.11, which uses Carrier Sense Multiple Access with Collision Avoidance(CSMA/CA). Every node has an identical radio communication component.

1. Simulation of TEAM

To evaluate system performance of TEAM protocol in terms of power efficiency, we simulate MANETs in a 300m $\times$ 300m area. Every node has a 250-meter maximum communication range. A pair of nodes are put on different sides of the network area as the source and the destination. Other nodes are distributed into the area uniformly. The number of nodes except the source and the destination varies from 2 to 60. We run an experiment 1000 times for each network scenario. We measure the aggregate transmission power consumption on TEAM paths and Minimum Transmission Power (MTP) paths. The ratios of the two values are listed in Table VI.

2. Simulation of TRUECON

We simulate the MANETs, which run TRUECON topology control algorithm, in a 600m $\times$ 600m area. Each node has a 150-meter maximum communication range. We put a pair of node on the different sides of the network area as the source and the destination. Each node runs TRUECON to adjust its transmission range. Then the source node starts a route discovery to find a path to the destination node. Two radio propagation models, free space model and two-ray ground reflection model, are

Table VI. THE POWER EFFICIENCY RATIO OF TEAM

Node Number	Mean	Max	Standard Deviation
2	1.001481	1.209226	0.000047
4	1.007567	1.449115	0.000239
6	1.018049	1.655392	0.000571
8	1.020374	1.541751	0.000644
10	1.0337	1.766807	0.001066
12	1.03882	1.690144	0.001228
14	1.045251	1.961561	0.009329
16	1.052269	1.932788	0.001653
18	1.058064	1.927126	0.001836
20	1.05592	1.789274	0.011528
22	1.061113	2.045898	0.000745
24	1.070623	1.789599	0.000108
26	1.068386	1.663842	0.001438
28	1.072929	2.081505	0.002306
30	1.074406	1.841529	0.002353
32	1.073218	1.964102	0.005993
34	1.078408	1.802884	0.002292
36	1.080445	1.774716	0.002544
38	1.087305	1.75219	0.002424
40	1.089756	2.1501	0.000766
42	1.083883	1.945597	0.004345
44	1.085873	1.91378	0.002716
46	1.092842	1.912383	0.005316
48	1.087426	1.841414	0.002765
50	1.094422	1.856569	0.000273
52	1.093925	2.200487	0.000841
54	1.098169	2.260616	0.007331
56	1.089928	1.771828	0.002957
58	1.103075	1.979415	0.002889
60	1.098718	2.222226	0.001073

Table VII. TRUECON SIMULATION RESULTS WITH FREE SPACE RADIO PROPAGATION MODEL

Nodes	Degree (TC)	Range (TC)	OP mean	OP std	Degree (W/o TC)	H ratio	H ratio std	C ratio mean	C ratio std
50	4.3012	89.9086	2.5863	0.2986	7.5336	1.0862	0.1356	1.0224	0.0327
60	4.645	85.0844	2.5952	0.2983	9.038	1.0686	0.0943	1.028	0.0449
70	4.9643	81.0842	2.6262	0.2873	10.7114	1.0486	0.1041	1.0209	0.0383
80	5.1273	77.1049	2.6343	0.2781	12.3263	1.0662	0.1042	1.0244	0.0346
90	5.1778	72.6729	2.6479	0.2849	13.8111	1.0758	0.1166	1.0265	0.0327
100	5.3032	70.3489	2.6817	0.2328	15.164	1.0835	0.1353	1.0266	0.0345
110	5.38	66.6618	2.6527	0.2116	16.9816	1.0849	0.1355	1.0263	0.0353
120	5.4468	64.3441	2.6527	0.2341	18.5752	1.0706	0.1250	1.0274	0.0339
130	5.4791	61.3267	2.687	0.2603	19.9782	1.0434	0.1027	1.0224	0.0267
140	5.5294	59.4496	2.7105	0.2341	21.5434	1.0579	0.1004	1.0199	0.0263
150	5.5073	57.1799	2.6435	0.2070	23.1573	1.0556	0.0800	1.0184	0.0221
160	5.5349	55.4419	2.6799	0.2203	24.8226	1.0465	0.0947	1.0216	0.0300
170	5.6201	54.3036	2.6644	0.2333	26.3169	1.0697	0.1124	1.0227	0.0237
180	5.6443	52.7324	2.6802	0.2139	27.7587	1.0639	0.1142	1.0197	0.0248
190	5.6473	51.3226	2.6831	0.2016	29.4097	1.0689	0.0988	1.0209	0.0218
200	5.7057	49.9998	2.726	0.2145	30.9918	1.0617	0.1032	1.019	0.0216
210	5.6567	48.7542	2.6844	0.1832	32.5615	1.0585	0.1026	1.0228	0.0288
220	5.7034	47.7384	2.6927	0.2348	34.2685	1.0666	0.1103	1.0243	0.0298
230	5.6916	46.6236	2.7111	0.2093	35.6128	1.0511	0.1014	1.021	0.0231
240	5.6758	45.5905	2.7262	0.2183	37.1722	1.0578	0.0827	1.0243	0.0277
250	5.7814	44.6707	2.7096	0.2035	38.8658	1.0537	0.0872	1.0246	0.0275
260	5.7685	43.9474	2.7233	0.2227	40.3744	1.0539	0.0861	1.0213	0.0224
270	5.7403	43.0789	2.7167	0.2033	42.0539	1.062	0.0853	1.0215	0.0220
280	5.7726	42.3318	2.7158	0.1963	43.5143	1.0681	0.1029	1.0242	0.0241
290	5.7606	41.5692	2.7183	0.1783	45.229	1.054	0.1010	1.0189	0.0206
300	5.8141	41.0218	2.693	0.1769	46.7325	1.0601	0.0942	1.0233	0.0283

used in the simulation respectively. We run an experiment 100 times for each network scenario.

We check the node degree and communication range of each node and calculate the aggregate transmission power on a path from the source to the destination before and after running TRUECON. The simulation results are displayed in Table VII, VIII. In the tables, 'OP' stands for overpayment; 'TC' denotes topology control; 'W/o TC' represents without topology control; 'H ratio' is the ratio of the hop numbers of the MTP paths before and after running TRUECON; 'C ratio' is the ratio of the aggregate transmission powers along the MTP paths before and after running TRUECON; 'std' means standard deviation.

Table VIII. TRUECON SIMULATION RESULTS WITH TWO-RAY RADIO PROPAGATION MODEL

Nodes	Degree (TC)	Range (TC)	OP mean	OP std	Degree (W/o TC)	H ratio	H ratio std	C ratio mean	C ratio std
50	4.3152	90.9437	5.79	1.8195	7.5008	1.0154	0.0606	1.003	0.0102
60	4.7173	86.6233	6.0033	1.5632	9.044	1.0101	0.0385	1.0079	0.0210
70	4.9214	81.0751	6.0643	1.4251	10.6146	1.0181	0.0567	1.0089	0.0288
80	5.0713	76.8649	6.0341	1.3928	12.2135	1.0091	0.0276	1.0046	0.0191
90	5.2516	73.3644	6.2396	1.3712	13.8782	1.0126	0.0427	1.0079	0.0244
100	5.3302	69.5836	6.3108	1.334	15.3358	1.0083	0.0451	1.0059	0.0151
110	5.3444	66.6718	6.2287	1.2669	16.7996	1.011	0.0273	1.005	0.0222
120	5.4662	64.1981	6.2367	1.5037	18.4012	1.0124	0.0409	1.0047	0.0163
130	5.5406	61.6315	6.3103	1.4066	20.0657	1.0052	0.0559	1.0036	0.0110
140	5.564	59.346	6.2935	1.214	21.6231	1.0123	0.0337	1.0063	0.0196
150	5.5807	57.8236	6.1407	1.143	23.0204	1.0108	0.0341	1.0068	0.0202
160	5.5641	55.6437	6.1468	1.0946	24.8904	1.0076	0.0277	1.0061	0.0164
170	5.5596	53.7645	6.3378	1.2404	26.3435	1.0259	0.0833	1.006	0.0127
180	5.6229	52.7089	6.5205	1.2235	27.598	1.0101	0.0368	1.005	0.0150
190	5.6597	51.3836	6.3701	1.0574	29.2351	1.0177	0.0394	1.0098	0.0224
200	5.6736	50.0838	6.1255	1.1652	30.8047	1.0041	0.0272	1.005	0.0181
210	5.7347	48.9786	6.431	1.106	32.7119	1.006	0.0308	1.0049	0.0159
220	5.6814	47.6265	6.545	1.0488	34.0149	1.007	0.0211	1.0046	0.0155
230	5.7254	46.7338	6.1591	1.1963	35.8143	1.0118	0.0369	1.0053	0.0179
240	5.7625	45.6311	6.2814	1.0714	37.164	1.0155	0.0634	1.0083	0.0449
250	5.73	44.8152	6.405	1.0065	38.7478	1.006	0.0231	1.0034	0.0103
260	5.7671	43.937	6.5299	1.0496	40.4423	1.0119	0.0365	1.0044	0.0101
270	5.773	43.0991	6.2772	1.0864	42.0253	1.0038	0.0523	1.0055	0.0141
280	5.8099	42.3433	6.4742	1.0844	43.5104	1.003	0.0552	1.0112	0.0522
290	5.7988	41.7672	6.4018	1.1614	44.8729	1.0024	0.0587	1.0057	0.0151
300	5.8221	40.9626	6.3434	1.0454	46.5068	1.0118	0.0301	1.0052	0.0130

Table IX. HEARING NODE NUMBER IN MANETS WITHOUT TOPOLOGY CONTROL

100		150		200		250		300	
mean	std	mean	std	mean	std	mean	std	mean	std
37.63	6.13	53.42	8.78	67.38	9.59	81.43	10.36	95.65	10.61

3. Simulation of Whisper

We simulate MANETs with Whisper routing protocol in a 600m $\times$ 600m area. Each nodes has a 150-meter maximum transmission range. We put a pair of nodes on the different sides of the network area as the source and the destination. Besides the source and destination nodes. Other network nodes are distributed uniformly into the area. We simulate the networks with 100, 150, 200, 250 and 300 nodes respectively. The forwarding probability of every node is varied from 0.1 to 0.9. As a reference, we also simulate AODV routing protocol for the same network scenarios as Whisper. For AODV, the forwarding probability of each node is zero and every node transmits with its maximum power. We run an experiment for 1000 times for each network scenario.

We measure the number of the nodes, which are able to hear the Route Request packet sent by the source initially. The path length of running Whisper is recorded and compared with the length of the path discovered by AODV. The total transmission power of the Whisper paths and the AODV paths are checked and compared. The simulation results are listed in Table IX, X, XI, XII, XIII. In the tables, 'std' denotes standard deviation; 'prob' represents forwarding probability.

Table X. HEARING NODE NUMBERS IN MANETS WITH TOPOLOGY CONTROL

	100 nodes		150 nodes		200 nodes		250 nodes		300 nodes	
prob	mean	std	mean	std	mean	std	mean	std	mean	std
0.1	22.55	5.11	27.92	5.88	31.66	6.15	35.54	6.51	38.57	6.75
0.2	22.67	5.11	27.57	5.71	31.92	6.43	35.71	6.66	38.40	6.77
0.3	22.66	5.0	27.59	5.80	31.92	6.23	35.50	6.74	38.96	6.95
0.4	22.86	5.04	28.14	5.74	32.37	6.41	35.87	6.56	38.81	6.56
0.5	22.85	5.30	28.12	5.75	32.19	6.17	35.99	6.53	38.95	6.69
0.6	23.30	5.12	28.22	5.85	32.80	6.48	36.49	6.72	39.37	6.96
0.7	23.38	5.23	28.49	5.73	32.87	6.35	36.85	6.76	39.69	6.90
0.8	23.84	5.40	29.11	6.23	33.25	6.46	37.02	6.97	39.73	7.00
0.9	23.96	5.08	29.69	6.12	33.54	6.74	37.58	7.04	41.18	7.25

Table XI. ROUTE LENGTH (HOPS) IN MANETS WITHOUT TOPOLOGY CONTROL

100		150		200		250		300	
mean	std	mean	std	mean	std	mean	std	mean	std
3.64	0.4906	3.43	0.4953	3.255	0.4361	3.144	0.3513	3.079	0.2699

Table XII. ROUTE LENGTH (HOPS) IN MANETS WITH TOPOLOGY CONTROL

	100 nodes		150 nodes		200 nodes		250 nodes		300 nodes	
prob	mean	std	mean	std	mean	std	mean	std	mean	std
0.1	7.73	1.3442	9.144	1.3947	10.419	1.4295	11.368	1.5182	12.403	1.5372
0.2	7.843	1.3565	9.267	1.3906	10.493	1.4967	11.6827	1.5682	12.4585	1.5884
0.3	8.021	1.4665	9.451	1.5518	10.729	1.6347	11.7267	1.7188	12.7477	1.6787
0.4	8.2623	1.6784	9.758	1.742	11.009	1.8681	11.993	1.844	13.0862	1.8447
0.5	8.5877	1.9583	10.003	2.0454	11.281	2.0259	12.32	2.1133	13.3347	2.1874
0.6	9.0823	2.316	10.5637	2.387	11.747	2.4643	12.8104	2.4811	13.7874	2.5052
0.7	9.8047	2.9692	11.2525	3.1238	12.5296	3.1087	13.7462	3.3303	14.6767	3.2719
0.8	11.3609	4.5486	12.8166	4.7352	14.0655	4.6275	15.5165	4.8689	16.4293	4.9866
0.9	16.3395	9.983	18.1506	9.6922	19.0244	9.3889	20.1348	9.5918	21.1101	9.3893

Table XIII. THE RATIO OF THE AGGREGATE POWER ON A ROUTE DISCOVERED BY WHISPER AND ON A ROUTE DISCOVERED BY AODV ROUTING PROTOCOL

	100 nodes		150 nodes		200 nodes		250 nodes		300 nodes	
prob	mean	std	mean	std	mean	std	mean	std	mean	std
0.1	0.6945	0.1454	0.5782	0.1085	0.5061	0.0921	0.4510	0.0753	0.4142	0.0676
0.2	0.7001	0.1387	0.5788	0.1108	0.5101	0.0962	0.4521	0.0769	0.4163	0.0676
0.3	0.6957	0.1444	0.5802	0.1151	0.5052	0.0906	0.4495	0.0737	0.4175	0.0695
0.4	0.7100	0.1535	0.5892	0.1200	0.5104	0.0951	0.4601	0.0788	0.4172	0.0664
0.5	0.72	0.1636	0.5862	0.1127	0.5163	0.0954	0.4638	0.0832	0.4212	0.0709
0.6	0.7283	0.1685	0.5990	0.1285	0.5255	0.0985	0.4678	0.0856	0.4240	0.0718
0.7	0.7393	0.1683	0.6090	0.1253	0.5336	0.1042	0.4759	0.0968	0.4309	0.0725
0.8	0.7693	0.1937	0.6284	0.1411	0.5435	0.1094	0.4863	0.0965	0.4423	0.0810
0.9	0.8685	0.3212	0.6942	0.2053	0.5878	0.1563	0.5220	0.1276	0.4798	0.1183

VITA

Jianfeng Cai received his B.E. in computer and software at the National University of Defense Technology, China in July 1994. He joined the Department of Computer Science at Texas A&M University in August 2000. His research interests include distributed systems and wireless mobile networking, especially resource management in ad hoc networks.

Mailing Address: 3366 Mt. Diablo Blvd. Apt. 205, Lafayette, CA 94549

The typist for this thesis was Jianfeng Cai.